managementnormen AKTUELL 01/2016

9. Mai 2016

Editorial

Der DIN-Normenausschuss Organisationsprozesse (NAOrg) wurde 2013 gegründet. Als Nachfolger der DIN-Koordinierungsstelle Managementsystemnormung (KoSMaS) ist er das zuständige Gremium für die Normung organisationsbezogener Prozesse auf nationaler, europäischer und internationaler Ebene. Erarbeitet werden Normen und Spezifikationen auf dem Gebiet der organisationsbezogenen Prozesse. Dies umfasst Managementsysteme, sofern diese nicht fach-/disziplinspezifisch sind und entsprechenden Gremien bereits zugeordnet sind oder werden können.

Der NAOrg ist ebenfalls zuständig für die strategische und inhaltliche Koordinierung der Arbeiten zum Thema Normung von Organisationsprozessen und Managementsystemen innerhalb von DIN. Dabei übernimmt er auch die Bewertung und Zuordnung neuer Normungsfelder in diesem Gebiet.

Der NAOrg besteht derzeit aus vier Arbeitsausschüssen zu den Themen Compliance-Management, Arbeitsschutzmanagementsysteme, Gesellschaftliche Verantwortung von Organisationen und Grundlagen des Risikomanagements.

Dieser Newsletter soll dazu dienen, über aktuelle, übergreifende Themen und Projekte der Normung im Bereich Organisationsprozesse und Managementsystemnormen zu informieren. In dieser Ausgabe berichten wir über die Revision der Norm ISO 31000 „Risikomanagement – Grundsätze und Leitlinien“, die Entwicklung der Normen ISO 19600 und ISO 37001 im Bereich Compliance-Management und den aktuellen Stand der Arbeiten an ISO 45001 „Arbeitsschutzmanagementsysteme – Anforderungen“.

Die Revision der ISO 31000 „Risikomanagement – Grundsätze und Leitlinien“

Die Norm ISO 31000 „Risk Management – Principles and Guidelines“, 2009 erschienen, wird derzeit in der Arbeitsgruppe 2 des zuständigen Technischen Komitees der ISO, dem ISO/TC 262 „Risk Management“, überarbeitet. Nachdem man sich zunächst an einer sogenannten „limited revision“ versucht hat, um ein schnelles Ergebnis zu erzielen, wurden die Grenzen aufgehoben, da die bloß geringfügigen Aktualisierungen aus Sicht der Mitglieder der Arbeitsgruppe keine Neuveröffentlichung rechtfertigten.

Die Grundstruktur der Norm soll stabil bleiben, um Endnutzern die erforderliche Sicherheit in der Anwendung zu bieten. Zugleich wird eine klarere Sprache und präzisere Anleitung der Nutzer angestrebt. Anforderungen an die Beachtung von menschlichen und kulturellen Faktoren sollen besser erläutert und Möglichkeiten für eine Reifegradmessung („Maturity Measurement“) angesprochen werden. Die Integration des Risikomanagements in alle organisatorischen Aktivitäten einschließlich der Entscheidungsfindung soll noch deutlicher herausgearbeitet werden. Damit werden zugleich die Anleitung für den risikobasierten Ansatz der Managementsystemnormen der ISO verbessert und Abstand von bloßem risikobasiertem Denken genommen.

Die Norm bleibt aller Voraussicht nach ein generisches Leitliniendokument mit den drei Säulen Prinzipien, Risikomanagementrahmen und Prozess und wird in dieser Revision nicht zu einer Managementsystemnorm Typ A oder Typ B weiterentwickelt. Auf nationaler Ebene wurde die Fassung 2009 nicht als DIN ISO – Norm übernommen, unter anderem, weil sie schon heute ein Managementsystem nahelege und damit die Gefahr gesehen wurde, dass ein ungewollter Zertifizierungsdruck entstehen könnte.

Worin also liegt der Nutzen der ISO 31000?

Diese Frage lässt sich leicht beantworten wenn man die integrale Struktur betrachtet. Die Überarbeitungen der in der Praxis oft angewendeten Managementsysteme für Qualität, Arbeitsschutz aber auch Umweltschutz zeigen den auf einem Risikomanagement basierenden Ansatz. Klare Forderungen aus diesen Normen sind die Identifika-

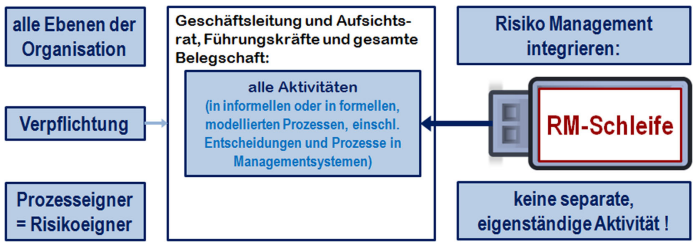
tion von Risiken, deren Beurteilung sowie die Bearbeitung und Umsetzung von Maßnahmen zu diesen Risiken. Das Ziel bleibt in all diesen Managementnormen gleich – ein verbessertes und risikoärmeres System. Hier genau bietet die ISO 31000 die Lösung. Durch ihren generischen Ansatz ist sie geeignet, auf alle Arten von Risiken angewendet zu werden. Insbesondere der im Kapitel 5 beschriebene Risikomanagementprozess eignet sich zur qualitativen oder quantitativen Beurteilung der Risiken. In diesem Zusammenhang sei die ebenfalls in der Überarbeitung befindliche ISO/IEC 31010 erwähnt, die eine Vielzahl von Risikobeurteilungsverfahren beschreibt.

Die ISO 31000, mehr als eine nützliche Umsetzungshilfe

Ein Blick in eine Organisation gleich welcher Größe, zeigt die Komplexität aller Aktivitäten und der dabei erforderlichen Entscheidungsfindung. Da sind gleich mehrere Managementsysteme, mit unterschiedlicher inhaltlicher Ausrichtung, wie Qualität, Umweltschutz, Arbeitsschutz oder Compliance und wahrscheinlich noch weitere. Alle diese Systeme können durch ein Risikomanagement nach ISO 31000 unterstützt werden. Ein Mehrwert allerdings wird durch das Zusammenspiel der Systeme bei der Entscheidungshilfe deutlich. Während die verschiedenen Managementsysteme in der Organisation nur geeignet sind, die jeweiligen Teilaspekte zu verbessern, gelingt durch einen integralen oder holistischen Ansatz - basierend auf einem Risikomanagementsystem - die Optimierung der Organisation als Ganzes. Dies gelingt durch die Beurteilung der verschiedenen Risiken mit gleicher Prozedur. Synergetische Aspekte der Maßnahmen werden deutlich und die Kommunikation komplexer Entscheidungen wird vereinfacht.

Risikomanagement – der „missing link“ zur Integration von Managementsystemen

Das Risikomanagement ist ein integraler Bestandteil aller organisatorischen Prozesse und keine Stand-alone-Aktivität, die von den wichtigsten Aktivitäten und Prozessen der Organisation getrennt bleibt. Es ist somit Teil der Aufgaben des Managements und der gesamten Belegschaft und in allen organisatorischen Prozessen, einschließlich der strategischen Planung und allen Projekt- und Change-Management-Prozessen vorhanden. Wie ein „Plug-In-Dongle“ verbessert es die Leistungsfähigkeit der Unternehmensprozesse:



Die Arbeiten an der ISO 31000 werden im DIN Normenausschuss Organisationsprozesse (NAOrg) und dort im Arbeitsausschuss „Grundlagen des Risikomanagements“ NA 175-00-04 AA begleitet. Dort werden derzeit auch in einer Taskgruppe die Vor- und Nachteile der Weiterentwicklung der Norm zu einer Managementsystemnorm untersucht, sowie in einer anderen Taskgruppe Überlegungen zu einer auf ISO 31000 beruhenden eigenständigen DIN-Norm zu Prinzipien und Prozessen des Risikomanagements angestellt.

(Autoren: Herr Prof. Dr. Udo Weis – Obmann des NA 175-00-04 AA, Herr Dr. Frank Herdmann – stellv. Obmann des NA 175-00-04 AA)

Entwicklung von Normen im Bereich Compliance-Management

Ein Leitfaden für Compliance

Im Juni 2012 reichte Australien bei ISO einen Vorschlag zur Erarbeitung einer Internationalen Norm zum Thema „Compliance Programs“ auf Basis der australischen Norm AS 3806 ein. DIN lehnte diesen Vorschlag zunächst ab, da der Zweck des Dokuments nicht klar war und ein möglicher Konflikt mit Gesetzen und bestehenden akzeptierten Initiativen (z.B. der OECD) zu drohen schien. Im Oktober 2012 nahmen die ISO-Mitglieder den Vorschlag allerdings mehrheitlich an und die Erarbeitung des Dokuments in einem neu gegründeten ISO-Projektkomitee unter australischer Leitung begann. Im Anschluss daran wurde auf deutscher Seite ein nationales Spiegelgremium bei DIN gegründet, um die Arbeiten von Anfang an beobachten und begleiten zu können. Auf der darauffolgenden internationalen Sitzung im Herbst 2013 konnten wesentliche deutsche Kommentare berücksichtigt werden, wie z. B. die weite Fassung einer Compliance-Funktion, die zuvor im nationalen Spiegelgremium erarbeitet wurde. Im Dezember 2014 wurde schließlich die ISO 19600 als Internationale Norm veröffentlicht. Das deutsche Spiegel-

gremium beschloss daraufhin Mitte 2015, die nationale Übernahme der ISO 19600 als DIN ISO-Norm. Ferner wurde in Abstimmung mit Österreich und der Schweiz beschlossen, eine gemeinsame deutsche Sprachfassung für den gesamten deutschen Sprachraum anzufertigen. Die Veröffentlichung der DIN ISO 19600 ist für Sommer 2016 vorgesehen.

Inhaltliche Besonderheiten der ISO 19600

Die ISO 19600 ist eine Typ-B-Managementsystem-Norm, welche Empfehlungen, jedoch keine Anforderungen enthält. Der Anwendungsbereich erstreckt sich über Organisationen und Unternehmen, im Besonderen auch über den Mittelstand. Die beinhalteten Grundsätze wie Flexibilität, Verhältnismäßigkeit oder auch Transparenz ermöglichen eine flexible Ausgestaltung der „Compliance Funktion".

Für die ISO 19600 kam die „High Level Structure" (HLS) für Managementsystemnormen zur Anwendung, die eine vergleichbare Gliederung und Struktur dieser Normen ermöglicht. Die Norm erklärt in logischer Abfolge, wie ein Compliance Management System (CMS) methodisch funktionieren kann. Dabei können die Unternehmen bzw. Anwender selbst entscheiden, wie sie die Empfehlungen der ISO 19600 für sich anpassen und umsetzen wollen.

Dies stellt auch einen wesentlichen Unterschied zum IDW PS 980 dar (in Deutschland bekannter Prüfstandard des Instituts der Deutschen Wirtschaftsprüfer für CMS), welcher den Fokus mehr auf die zu prüfende Seite legt und die Grundsätze für Wirtschaftsprüfer aufstellt.

Die ISO 19600 dagegen gibt dem CMS-Verantwortlichen klare Empfehlungen, wie ein CMS einzuführen, durchzuführen und auszugestalten ist, um Wirksamkeit im Unternehmen zu entfalten. Daraus folgen ein sich ergänzender Ansatz beider Standards und ein großer Mehrwert für den Anwender.

Gelten weltweit gleiche Compliance-Standards, kann dies operative Geschäfte international tätiger Unternehmen erheblich beschleunigen und auch insbesondere für global handelnde Unternehmen sowie den Mittelstand einen erheblichen Vorteil darstellen.

Entstehung der ISO 37001 „Anti-bribery management systems"

Im Oktober 2012 reichte Großbritannien bei ISO einen Vorschlag zur Erarbeitung einer Internationalen Norm zum Thema „Anti-bribery management systems" auf Basis der britischen Norm BS 10500 ein. Auch hier lehnte DIN den Vorschlag zuerst ab, da eine weite Überschneidung mit gesetzlichen Regelungen und Risikomanagementsystemen gesehen wurde. Im Februar 2013 nahmen jedoch die ISO-Mitglieder den Vorschlag mehrheitlich an, was auch hier zu der Gründung eines neuen ISO-Projektkomitees, diesmal unter britischer Leitung, führte. Die deutsche Mitarbeit wurde hier von Anfang an im gleichen nationalen Spiegelgremium des NAOrg koordiniert, welches auch bereits die Arbeiten an ISO 19600 begleitete.

Spannungsfeld ISO 19600 und ISO 37001

Am Anfang des Erarbeitungsprozesses der ISO 37001 wurde auf internationaler Ebene beschlossen, diese Norm als eine Typ-A-Managementsystemnorm zu entwickeln, d.h. nicht nur mit Empfehlungen sondern klaren Anforderungen auszustatten. Die ISO 37001 folgt ebenfalls der HLS und ist somit, wie auch die ISO 19600, modular im Unternehmen zu handhaben.

Eine Managementsystemnorm zur Steuerung von Korruptionsrisiken als eine Untermenge von Compliance Risiken hält natürlich vergleichbare Elemente und Prozesse bereit, die auch bereits ISO 19600 vorsieht. Aus deutscher Sicht gilt es nun, einen Konflikt aufgrund von Überschneidungen von Funktionen und Prozessen mit der ISO 19600 zu vermeiden und eine Angleichung der Terminologie anzustreben. Dazu halten wir dieses wichtige Anliegen auch stets auf der Agenda und haben in kleineren Arbeitsgruppen auf internationaler Bühne bisher stetig nachgehalten. Eine notwendige Synchronisierung mit der ISO 19600 befindet sich deshalb auf einem guten Wege, was am Ende zu einer sinnvollen Anwendung beider Normen führen wird.

Derzeit steht die internationale Diskussion der während der Entwurfsumfrage eingegangenen Kommentare zu ISO 37001 (ca. 550) bevor. In Deutschland wurde der Entwurf E DIN ISO 37001 zur Stellungnahme von Januar 2016 bis März 2016 veröffentlicht. Eine Veröffentlichung der fertigen ISO 37001 kann in Abhängigkeit von den Resultaten der bevorstehenden internationalen Diskussionen für Ende 2016 bzw. Anfang 2017 erwartet werden.

Aktueller Stand der Arbeiten zu ISO 45001 „Arbeitsschutzmanagement-systeme – Anforderungen“

Im Projektkomitee ISO/PC 283 mit britischem Sekretariat wird derzeit die ISO 45001 "Arbeitsschutzmanagement-systeme - Anforderungen mit Leitlinien zur Anwendung“ erarbeitet. Zu diesem Thema existierte bislang keine ISO-Norm, jedoch der weit verbreitete Standard OHSAS 18001, der die Basis für die inhaltliche Arbeit bildet.

Nachdem zunächst ein Arbeitsentwurf vorgelegt wurde, erarbeitete das ISO/PC 283 auf Grundlage der sehr zahlreich eingegangenen Kommentare einen ersten Komitee-Entwurf. Zu diesem gingen wiederum mehr als 2400 Einzelkommentare ein, die im Rahmen von zwei Sitzungen beraten wurden und in einem zweiten Komitee-Entwurf resultierten. Nach abschließender Beratung der ebenfalls sehr zahlreich eingegangenen Kommentare zum zweiten Komitee-Entwurf, beschloss das ISO/PC 283 im September 2015, dass das überarbeitete Dokument die Entwurfsreife (DIS) erreicht hat.

Das zuständige deutsche Spiegelgremium NA 175-00-02 AA im DIN-Normenausschuss Organisationsprozesse (NAOrg) beschloss in seiner Sitzung im Dezember 2015 die unveränderte Übernahme des ISO-Projekts als DIN ISO 45001. Begleitend zur ISO-Umfrage sollte auch ein nationaler Entwurf als zweisprachige Ausgabe veröffentlicht werden. Im März 2016 wurde daher die E DIN ISO 45001 "Arbeitsschutzmanagementsysteme - Anforderungen mit Leitlinien zur Anwendung (ISO/DIS 45001:2016)" veröffentlicht. Nach Abschluss der ISO-Umfrage am 13. Mai 2016 werden im Rahmen weiterer Sitzungen des ISO/PC 283 die eingegangenen Kommentare behandelt.

Nach derzeitigem Kenntnisstand ist die Veröffentlichung der ISO 45001 erst im Jahr 2017 zu erwarten.

Haben Sie Fragen zu den Arbeiten im Normenausschuss Organisationsprozesse (NAOrg) oder Interesse an einer Mitarbeit? Dann sprechen Sie uns an:

Ansprechpartner NAOrg:

Geschäftsführer: Reiner Hager
Teamkoordinator: Stefan Holzapfel

DIN Deutsches Institut für Normung e. V.
Normenausschuss Organisationsprozesse (NAOrg)

Tel.: 030 2601-2187 (Herr Holzapfel)
E-Mail: naorg@din.de
Web: www.din.de/go/naorg