43. Jahrgang CHF 14.30 / € 13,50 ISSN 1862-2623

MQ Management und Qualität

Ausgabe 12/2013

Das Magazin für integrierte Managementsysteme

Seite 4
Wohin die Reise geht

Basis für Nachhaltigkeit

MQ Die Königsdisziplin – In Projekten führen

Maturity Models im Risikomanagement

Implementierung von ISO 31000:2009

Von Heinrich Kuhn

Der ISO-Standard 31000:2009 hat sich im Risikomanagement in den letzten Jahren rasch als anerkannter Benchmark etabliert. Viele Unternehmen haben die Vorteile der ISO 31000:2009 für das Risikomanagement erkannt. Aber die Implementierung ist anspruchsvoll. Maturity Models sind eine gute methodische Grundlage, um diese Herausforderung erfolgreich zu meistern.

Im Risikomanagement hat in den letzten zehn Jahren eine sehr dynamische Entwicklung stattgefunden, insbesondere in den letzten fünf Jahren. Bis 2009 gab es keinen internationalen ISO-Standard im Risikomanagement. Sehr oft war das Risikomanagement in Unternehmen eine Landschaft von Insellösungen: Neben den gesetzlich vorgeschriebenen Risikobereichen Arbeits-, Produkte- und Prozesssicherheit existierte ein Risikomanagement im operativen Bereich, das in der Regel eine Unternehmensinterne Lösung war. Bei grösseren Unternehmen wurde zusätzlich noch ein COSO-Ansatz parallel geführt. Eine einheitliche Erfassung, Bewertung und Aggregation der Unternehmensrisiken wurde dadurch sehr erschwert resp. verunmöglicht. Die Integration der unterschiedlichen Risikodaten war oft ein Desiderat, aber nicht die Realität. Die ISO 31000:2009 hat diese Problematik erfolgreich gelöst.

Generischer RM-Standard

Probleme der Implementierung

Rasch wurden der Nutzen und die Bedeutung erkannt, dass das Risikomanagement auf der Grundlage von ISO 31000:2009 mit anderen Managementsystemen (zum Beispiel ISO 9000, ISO 14000, HSE [Health, Safety & Environment]) sehr gut in einem Gesamtmanagementsystem integriert werden kann. Allerdings gab es eine Schwierigkeit: Das Delta zwischen dem ursprünglichen, einfachen Risikomanagement, welches in Unternehmen implementiert war, und dem Gesamtansatz von ISO 31000:2009 war oft recht gross. Diese Problematik führte immer wieder dazu, dass der neue Standard nicht eingeführt wurde.

Einen wichtigen methodischen Lösungsansatz für diese Problemstellung im Risikomanagement liefern Maturity Models. Die Grundidee des Maturity Models ist, dass die Entwicklung und Implementierung von Risikomanagement-Systemen stufenweise vorgenommen wird. Genau wie es im Alltag wichtig ist, dass Treppen Höhendifferenzen überwinden helfen, ist es bei Maturity Models: Sie müssen in die richtige Richtung angelegt sein und auch die richtige Stufenhöhe aufweisen.

Richtung und Stufenhöhe

Maturity Models: alte Bekannte

Dieser methodische Ansatz findet sich in sehr unterschiedlichen Bereichen wie etwa beim Safety- und Security-Management und beim Projekt- und Qualitätsmanagement. Auch im Umfeld der internen und externen Revision sind Maturity Models sehr verbreitet, so zum Beispiel beim Internen Kontrollsystem (IKS). Insofern handelt es sich um einen bekannten und erprobten methodischen Ansatz.

Die Entwicklung der ISO 31000:2009 wurde sehr stark durch den australisch-neuseeländischen Standard AS/NZ 4360:2004 geprägt. Der nationale Standard war im ganzen angelsächsischen Bereich der Referenzstandard im Risikomanagement. Dieser Vorsprung findet sich auch heute noch bei den nationalen «Implementation Guidelines» zur ISO 31000:2009 und insbesondere auch beim Einsatz vom Maturity Modelen im Risikomanagement. Stellvertretend seien folgende nationale «Implementation Guidelines» erwähnt:

- Grossbritannien: BS 31100:2011: Risk management. Code of practice and guidance for the implementation of BS ISO 31000
- Kanada: Q31001-11 – Implementation guide to CAN/CSA-ISO 31000, Risk management – Principles and guidelines
- Australien: HB 158-2010: Delivering assurance based on ISO 31000:2009 – Risk management – Principles and guidelines.

Da Maturity Models im Risikomanagement oft die grossen «bekannten Unbekannten» sind, lohnt es sich, sich zu überlegen, welchen konkreten Nutzen Maturity Models im Risikomanagement haben. Es sind insbesondere drei Nutzenpotenziale, die durch Maturity Models aktiviert werden:

1. Massgeschneidertes Risikomanagement

Eine wichtiger Grundsatz der ISO 31000:2009 ist, dass jedes Risikomanagement-System «massgeschneidert» sein soll: «risk ma-

Heinrich Kuhn, ZHAW, School of Engineering, Institut für Nachhaltige Entwicklung (INE), Professor für Integriertes Risikomanagement im MAS in Integrated Risk Management; Mitglied der Spiegelkomitees ISO/SNV für Risikomanagement (TC 262: ISO 31004) und BCM (TC 223: ISO 22300ff.); heinrich.kuhn@zhaw.ch

Risk Management Attribute Grafik 1

Risk-Management-Eigenschaften	Maturity Level – Basic	Maturity Level – Mature	Maturity Level – Advanced
Maturity-Beschreibung	Die Organisation erfüllt grundlegende interne und externe Stakeholder-Risikomanagement-Erwartungen aus einer Compliance-Perspektive.	Aktivitäten und Techniken für ein umfassenderes Vertrauen der Stakeholder werden eingesetzt, um Risiken proaktiv zu managen. Die Integration von Risiko-Management-Aktivitäten erfolgt über die (ganze) Organisation.	Risikomanagement wird als strategisches Instrument gesehen, um die Performance zu verbessern und gehört zu den Grundwerten der Organisation.
Governance & Accessibility	Es existieren Risikomanagement-Policies und Verfahren, um die Compliance und die interne Kontrolle zu erfüllen.	Es existieren ein RM-Framework und eine Governance-Struktur mit klaren Verantwortlichkeiten (accountabilities), um die Ziele des Risikomanagements zu unterstützen.	Die Verantwortung (accountability) im Risikomanagement ist voll mit Performance-Management integriert.
Decision-Making	Die Entscheidungsprozesse werden durch spezifische oder hoch spezialisierte Risikoanalysen auf der funktionalen Ebene unterstützt.	Wichtige Finanz-, Betriebs-, Technologie- und Change-Management-Entscheidungen werden durch Risikobeurteilungen unterstützt. Risiko- und Kontroll-Aktivitäten werden in die Geschäftsprozesse eingebettet.	Die Organisation führt die Beurteilung von strategischen Risiken, von Geschäftseinheiten oder operationellen Risiken und von grossen Investitionen oder Projekten durch. Das Verfahren der Risikobeurteilung ist auf die mehrjährige strategische Planung und auf die jährlichen Unternehmensplanungszyklen ausgerichtet.
Risk Management und Optimierung	Auf der Grundlage einer organisationsweiten Perspektive gibt es funktionale Risikobewertungen mit einem spezifischen Analyse- und Interpretationsansatz.	In Übereinstimmung mit den normalen Management-Analysen und dem Reporting kommen häufige Risikobewertungen vor. Die Risiken werden beurteilt und in einer integrierten Art und Weise in der gesamten Organisation gemanagt.	Die Organisation führt die Beurteilung von strategischen Risiken, von Geschäftseinheiten oder operationellen Risiken und von grossen Investitionen oder Projekten durch. Das Verfahren der Risikobeurteilung ist auf die mehrjährige strategische Planung und auf die jährlichen Unternehmensplanung Zyklen ausgerichtet.
Kommunikation und Reporting	Business Risk Reporting ist in erster Linie darauf ausgerichtet, die externe Berichterstattung oder die Compliance-Anforderungen zu unterstützen.	Es gibt eine umfangreiche Berichterstattung an die Geschäftsleitung oder den Vorstand, an das Audit-Komitee und für die wichtigsten Stakeholder in Bezug auf die aktuellen Risiko-Levels und die zukünftigen Risiko-Themen.	Es gibt eine unternehmensweite Analyse, Aggregation und ein Reporting über alle Risikobereiche. Unterstützt wird dies durch spezialisierte Risikomanagement-Informationssysteme. Alle Risiko-Reportings werden aufeinander ausgerichtet, um eine umfassende Top-down- und Bottom-up-Sicht auf die Risiken zu ermöglichen.
Performance Assessment & kontinuierliche Verbessung	Performance Assessment ist mit funktionellen oder hoch spezialisierten Risikomanagement-Aufgaben verbunden.	Die expliziten Anforderungen für das RM Performance Assessment sind auf die Governance- und die Rechenschaftspflicht-Struktur ausgerichtet. Es gibt eine regelmässige und unabhängige Evaluation des Risiko-Management-Frameworks, der RM-Policies, der Verfahren und der Mitarbeiter. Es existiert ein mehrjähriges Programm zur kontinuierlichen Verbesserung.	Es existiert eine risikoüberwachte Strategie in Bezug auf die Performance-Bewertung und die Ressourcen-Allokation.

nagement is tailored» (Principle 7, ISO 31000:2009). Dieser Grundsatz wird einerseits dadurch eingelöst, dass die Risikodefinition nach ISO 31000:2009 sich explizit auf die internen und externen Unternehmensziele fokussiert. Der Fokus der Risikobewertung umfasst somit also auch die Stakeholder mit ihren teilweise divergierenden Erwartungen.

Da diese erweiterte Perspektive komplex und anspruchsvoll sein kann, ist es zwingend notwendig, sich zu überlegen, wie das Risikomanagement zielführend implementiert werden kann. Maturity Models ermöglichen es, diese Aufgabenstellung gut umzusetzen.

Bei einer solchen Implementierung geht es nicht darum, dass alle Unternehmensbereiche zur höchsten RM-Stufe geführt werden, sondern auch hier gilt, dass Risikomanagement «massgeschneidert» sein soll. Bei einem fünfstufigen Maturity Model kann

Dreifacher Nutzen

es durchaus sein, dass gewisse Unternehmensbereiche auf Stufe 4 verbleiben können, in gewissen Fällen sogar auf Stufe 3.

2. Messbarkeit, Vergleichbarkeit und Konsistenz

Durch das Maturity Model wird ermöglicht, dass die Implementierung eines Risikomanagement-Systems mess- und vergleichbar wird. Im RM-Prozess von ISO 31000 ist der Parallelprozess «Monitor und Review» darum sehr wichtig. Nur mit diesem Ansatz kann das Risikomanagement im Unternehmen längerfristig seine Bedeutung und auch Legitimation behalten. Last, but not least ermöglicht ein Maturity Model die Beurteilung, ob ein Risikomanagement in sich konsistent ist. Es verhindert somit, dass das Risikomanagement im Laufe der Zeit zu einem Patchwork wird, wie das früher oft der Fall war.

3. Implementierung und Investition

Risikomanagement ist für jedes Unternehmen immer auch eine Investition. In Zeiten der knappen finanziellen und zeitlichen Res-

sourcen ist es besonders wichtig, mit einem Konzept zu arbeiten, das sinnvolle und praktikable Implementierungsschritte aufweist.

Zuerst können zum Beispiel die Risiken erfasst und bewältigt werden, die dringlich und auch wichtig sind. Auf der Grundlage solcher «Quick Wins» wird ersichtlich, was der konkrete Nutzen eines Risikomanagements ist. Die Freigabe für die nächsten Maturity-Model-Stufen wird dadurch begünstigt.

Methodik

Maturity Models verfolgen das Ziel, auf der Grundlage von definierten RM-Schwerpunkten aufzuzeigen, wie diese stufenweise implementiert werden können. Diese Schwerpunkte werden mittels Risiko-Eigenschaften (risk attributes) genauer charakterisiert.
Wichtig bei solchen Maturity Models ist, dass die Wahl dieser Risiko-Eigenschaften und die Wahl des Maturity Models, im Regelfall mit drei bis max. zehn Stufen, eine konzeptionelle Arbeit des/der verantwortlichen Risikomanagers/in ist. Nur wenn die Risk Attributes optimal auf die spezifischen Vorgaben und Ziele eines Unternehmens abgestimmt werden, ist das Maturity Model ein zielführendes Instrument.

Viele nationale «Implementation Guidelines» zur ISO 31000:2009 enthalten Maturity Models, die aber in jedem Fall adaptiert werden müssen. Ein einfaches Beispiel eines solchen Maturity Models findet sich im Draft des kanadischen Standards «Q31001-11 – Implementation guide to CAN/CSA-ISO 31000, Risk management – Principles and guidelines» (vgl. Grafik 1).

Dieses Beispiel mit drei Maturity-Stufen ist die einfachste mögliche Konkretisierung. In vielen Fällen kommt ein fünfstufiges Modell zum Einsatz. Dieses erweiterte Modell erlaubt durch die grössere Granularität eine genauere Aussage im Bezug auf den Maturitäts-Level. Die fünf Levels werden wie folgt definiert:

1. Inital
2. Repeatable
3. Defined
4. Managed
5. Optimized

Wie für die ISO 31000:2009 allgemein gilt bei einem Maturity Model ganz besonders: Risikomanagement ist massgeschneidert. Nur dann ist es auch wirkungsorientiert.

Trends im Risikomanagement

Das Institut of Internal Auditors (IIA) hat in den letzten Jahren sehr interessante Publikationen zum Risikomanagement veröffentlicht, die aufzeigen, wie Risikomanagement nach ISO 31000:2009 und Internes Audit aufeinander abgestimmt werden können. Dabei spielen Maturity Models eine zentrale Rolle. Durch diese gegenseitige Bezugnahme wird die Relevanz der ISO 31000:2009 klar gestärkt.

Seit 2012 ist eine grössere Anzahl Standards im BCM (Business Continuity Management) erschienen, so zum Beispiel die ISO 22301:2012. Dieser neue BCM-Standard ist mit der ISO 31000:2009 vollständig abgeglichen worden. Das zeigt sich nicht nur bei den Definitionen und wichtigen Schnittstellen, sondern auch beim Einsatz von Maturity Models.

Zusammenfassend kann festgehalten werden, dass in Zukunft sowohl im Risikomanagement als auch im BCM und im Internen Kontrollsystem (IKS) der methodische Ansatz der Maturity Models immer mehr zu einem entscheidenden Erfolgsfaktor bei der Implementierung werden wird. ■