DR. FRANK HERDMANN RECHTSANWALT
AUXILIUM MANAGEMENT SERVICE

Die Grundlagen des Risikomanagements und der risikobasierte Ansatz in den Managementsystemnormen von DIN und ISO

Risikomanagement – Historischer Kontext:
Betriebswirtschaftlehre im 20. Jahrhundert

Risiko wird zusammen mit der Ungewissheit als Grundproblem der Planung bewertet und zum Thema der Entscheidungsregeln gemacht (Wöhe, 13. Auflage 1978, S. 130/133)

vollkommene Information ⟷ **unvollkommene Information** ⟷ **vollkommene Ignoranz**

Entscheidungssituationen		
Sicherheit	**Risiko**	**Unsicherheit**
einwertige Erwartungen	einwertige Erwartungen	mehrwertige Erwartungen
einwertige Wahrscheinlichkeiten	mehrwertige Wahrscheinlichkeiten	mehrwertige Wahrscheinlichkeiten, gar keine Wahrscheinlichkeit

Da es allgemeine Entscheidungsregeln bei unvollkommener Information (noch) nicht gibt, ist das Resultat für die Praxis die Notwendigkeit der **Flexibilität der Planung**.

Risikomanagement – Historischer Kontext:
Zeitalter der Managementsysteme

- Vor 1990 hatten nur wenige Wirtschaftsbereiche zumeist rechtlich vorgegebene und aus dem Aspekt der Sicherheit entwickelte Systematiken zur Risikokontrolle.
- Komplexere Strukturen und Verfahren, rascher technologischer Fortschritt und sinkende Lebenszyklen von Produkten und Dienstleistungen ➨ prozessorientierte Sicht auf die Tätigkeit von Unternehmen (W.E Deming; PDCA-Zyklus – Plan-Do-Check-Act)

  ➨ Entwicklung immer neuer Managementsysteme [Schools (Churches) of Management]
- I.d.R. haben alle Managementsysteme einen mit dem PDCA-Zyklus vergleichbaren Aufbau: auf Basis vorhandener Erfahrungen sind im Rahmen einer Analyse Abweichungen vom normalen Betrieb festzustellen und zu korrigieren.

Risikomanagement nach ISO 31000 kann als Bindeglied aller Managementsysteme verstanden werden.

ISO 31000 strebt nicht nur die nachsorgende, sondern auch die vorsorgende Betrachtung in Prozessen und Verfahren an ➨ Nutzen im Alltag der wertorientierten Unternehmensleitung !

Risikomanagement – Rechtlicher Kontext:
Gesetz zur Kontrolle und Transparenz im Unternehmensbereich

- **KonTraG** seit 1. Mai 1998 in Kraft
- Vorstände von Aktiengesellschaften sind verpflichtet, ein Überwachungssystem einzurichten ➡ neuer Stellenwert für das Risikomanagement
- Ziel: bestandsgefährdende Entwicklungen früh (?) erkennen
- Notwendigkeit, die Ablaufprozesse und Organisationsstrukturen auf Risiken zu prüfen (siehe Gesetzesbegründung)
- Der Vorstand muss in einer Unternehmenskrise nachweisen, dass er alle erforderlichen Maßnahmen zur Risikofrüherkennung und -abwehr getroffen hat (Abwehr der Haftung wegen Organisationsverschuldens).
- Anforderungen an das Risikofrüherkennungs- und -überwachungssystem: IDW PS 340 (ggf. Prüfungsumfang nach § 317, Abs. 4 HGB!)

Andere Gesellschaftsformen: Ausdehnung des Anwendungsbereiches dieser Regeln durch

- die allgemeinen Regeln zur Haftung wegen Organisationsverschuldens (Austrahlungswirkung auf den Pflichtenrahmen des Geschäftsführers)
- Gesellschaftssatzungen und Gesellschafterbeschlüsse

Risikomanagement – Rechtlicher Kontext: Weitere Normen

Bilanzrechtsreformgesetz (BilReG):

- Kapitalgesellschaften
- Beurteilung und Erläuterung der voraussichtlichen Entwicklung mit ihren wesentlichen Chancen und Risiken (§ 289, Abs. 1 HGB)

Bilanzrechtsmodernisierungsgesetz (BilMoG) vom Mai 2009:

- Beschreibung der wesentlichen Merkmale des internen Kontroll- und Risikomanagementsystems im Hinblick auf den Rechnungslegungsprozess im Lagebericht von kapitalmarktorientierten Kapitalgesellschaften (§ 289, Abs. 5 HBG)

Kreditwesengesetz (KWG):

- Kreditinstitute
- Offenlegung der wirtschaftlichen Verhältnisse der Kreditnehmer für Kredite über 250 TEUR nach § 18 Satz 1 KWG
- I.d.R. Vorlage geprüfter Jahresabschlüsse (incl. Prüfung und Kommentierung, ob das Risikomanagementsystem den Anforderungen des Unternehmens entspricht)

Risikomanagement – Rechtlicher Kontext:
MaRisk [Rundschreiben 10/2012 (BA) der BaFin]

Basierend auf § 25 a Abs. 1 KWG hat die Bundesanstalt für Finanzdienstleistungsaufsicht mit Rundschreiben die Mindestanforderungen an das Risikomanagement (MaRisk) für Kreditinstitute beschrieben.

Das Gesetz verlange eine ordnungsgemäße Geschäftsorganisation, die … die betriebswirtschaftlichen Notwendigkeiten gewährleistet. Dazu gehöre insbesondere ein angemessenes und wirksames Risikomanagement.

Das Risikomanagement beinhalte nach dem Gesetz:

- die Festlegung von Strategien, Verfahren zur Ermittlung und die Sicherstellung der Risikotragfähigkeit sowie
- die Einrichtung interner Kontrollverfahren mit
  - einem internen Kontrollsystem und
  - einer Internen Revision

Die Ausgestaltung des Risikomanagements hänge von Art, Umfang, Komplexität und Risikogehalt der Geschäftstätigkeit ab. (Austrahlungswirkung?)

Internationale Standards und Normen
Beispiele

- **AS NZS 4360:1995** Risk Management Standard, Australien & Neuseeland 1995 (inzwischen ersetzt duch AS NZS 31000: 2009)
- **CAN/CSA Q850** Risk Management: Guideline for Decision-Makers (Kanada 1997)
- **BS-6079-3:2000** Project management. Guide to the management of business related project risk (Großbritannien 2000)
- **COSO ERM** Enterprise Risk Management - Integrated Framework (USA 2004)
- **ONR 49000:2004 ff.** Risikomanagement für Organisationen und Systeme: Begriffe und Grundlagen (Österreich 2004)
- **ISO Guide 73:2009** Risk Management – Vocabulary (international 13. Nov. 2009)
- **ISO 31000:2009** Risk Management – Principles and guidelines (international, 15. Nov. 2009)
- **ISO/TR 31004:2013** Risk Management Guidance for the implementation of ISO 31000 (international 2013)
- **IEC/ISO 31010:2010** Risk management - Risk assessment techniques (CENELEC, 01.05.2010)

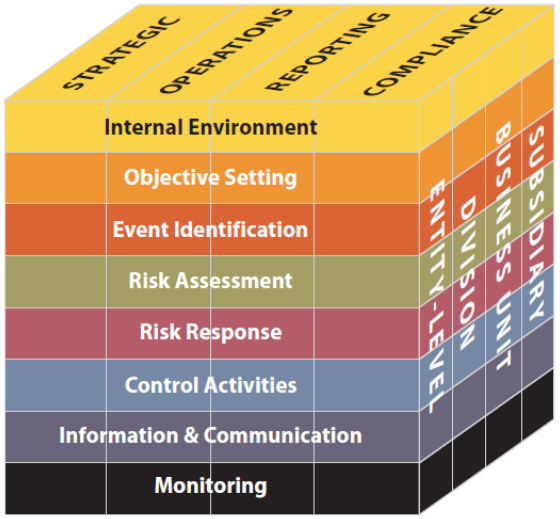
Die Aufzählung ist beispielhaft und nicht vollständig!

- **E DIN ISO 31000:2011-01** (deutscher Normentwurf nebst nationalem Vorwort und nationalen Fußnoten) wurde zurückgezogen
  (Zusammenfassung dazu bei Herdmann, **ISO 31000 and DIN:** http://herdmann.de/publikationen/index.php)

Internationale Standards und Normen
COSO ERM

Die Buchstaben »C O S O« stehen für das »Committee of Sponsoring Organizations of the Treadway Commission«. COSO veröffentlichte zunächst das Rahmenmodell »Internal Control – Integrated Framework (1992)« (»COSO IC«) – eine Anleitung für Unternehmensleiter zur Strukturierung und Einführung **interner Kontrollen**, um die Unternehmensziele in Bezug auf Operations, Reporting und **Compliance** zur erreichen. COSO-IC wurde 2002 mit Section 404 des Sarbanes / Oxley Act (nachfolgend »SOx 404«) zur festen Größe in amerikanischen Unternehmen und in der Prüfungsrichtlinie Nr. 2 des »Public Company Accounting Oversight Board« zum offiziellen Referenzmodell.

Als Weiterentwicklung wurde 2004 »COSO ERM« als Risikomanagement-Rahmenmodell veröffentlicht und bildet den wesentlichen Teil der Corporate Governance. International galt das amerikanische Rahmenmodell »COSO ERM« (Enterprise Risk Management – Integrated Framework) lange als führendes Referenzmodell für Wirtschaftsprüfer.



ERM-Würfel aus: Enterprise Risk Management – Integrated Framework; Executive Summary; PWC für COSO; Jersey City, NJ 2004 als Download im Internet unter:

http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf

Internationale Standards und Normen
ONR 49000

- integrierter Managementansatz auf Basis des PDCA (plan-do-check-act Zyklus) aufgrund der Überschneidungen mit anderen Managementsystemen: Verpflichtung zur Integration des Risikomanagements in die anderen Führungssysteme des Unternehmens
- Verpflichtung zur Benennung eines Risikoverantwortlichen und zur Bereitstellung erforderlicher Ressourcen
- Identifikation und quantitative Bewertung der Risiken und ihrer Interdependenzen erforderlich sowie Bestimmung des Gesamtrisikoumfangs und des benötigten Risikokapitals
- Risikobewältigung und kontinuierliche Risikoüberwachung
- Dokumentation

Nähe zu IDW PS 340 wird gesehen.

Die Prinzipien des ONR 49000 und der ISO 31000 sollen im Einklang stehen (aber: externe Begutachtung und Zertifizierung!); ONR verwendet die Definitionen des ISO Guide 73:2009

Internationale Standards und Normen
ISO 31000 – Gliederung

- Foreword (Vorwort)
- Introduction (Einleitung)
- **1 – Scope** (Anwendungsbereich)
- **2 – Terms and definitions** (Begriffe)
- **3 – Principles** (Grundsätze)
- **4 – Framework** (Risikomangementrahmen)
- **5 – Process** (Prozess)
- Annex A (Informative) Merkmale eines erweiterten Risikomanagements
- Bibliography (Literaturhinweise) ➨ ISO Guide 73:2009 & ISO/IEC 31010

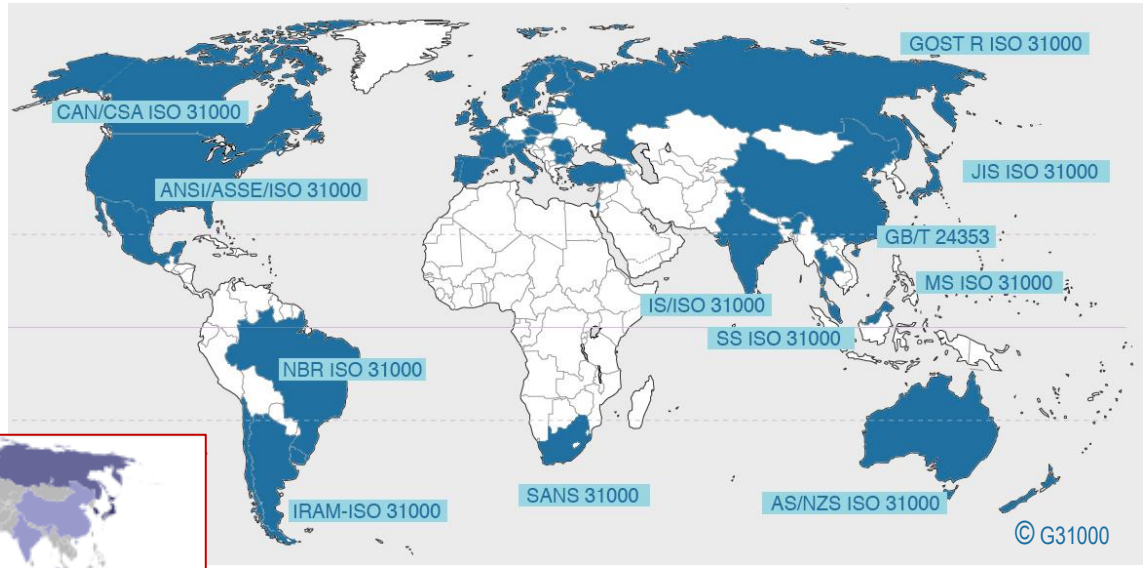
(in Klammern die in »**E DIN ISO 31000-2011-01**« verwendeten Begriffe)

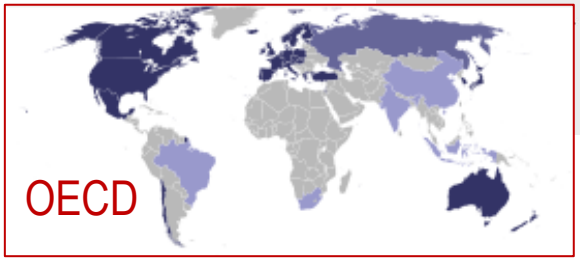
Weiter Anwendungsbereich:

- alle Formen von Organisationen
- in allen Wirtschaftszweigen

Internationale Standards und Normen
ISO 31000:2009 – Bedeutung und Ziele

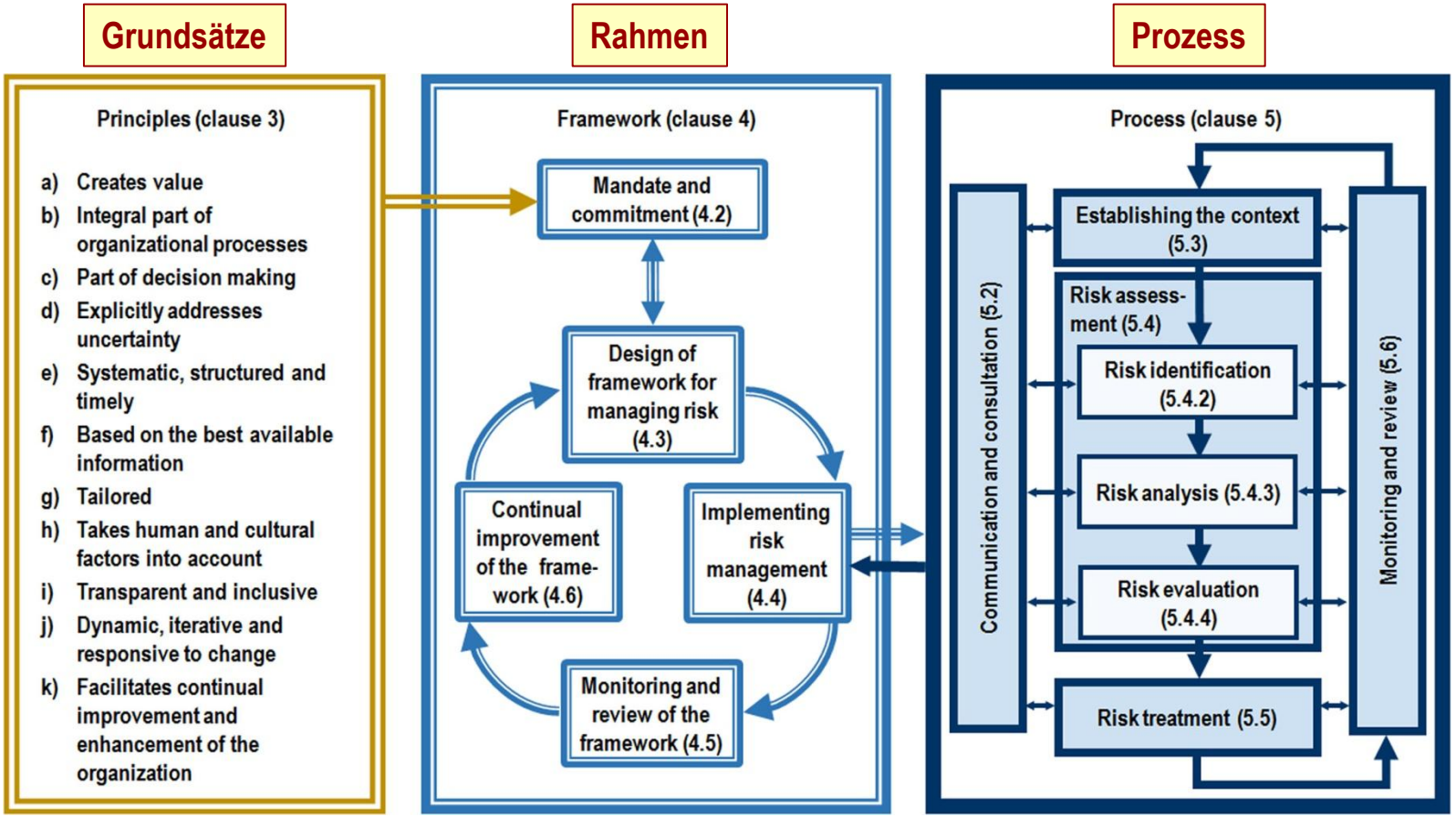
- Kurzer und klarer Text, nicht radikal neu (common sense)
- Maßgeschneidertes Risikomanagement verlangt
  - ➨ kann (z.B. bei KMU) vereinfacht werden
- Generische Rahmenrichtlinien statt einheitliches (uniformes) Risikomanagement
- Dient ausdrücklich nicht der Zertifizierung
- Internationaler Konsens
- Hoher Verbreitungsgrad
- Weltweite Referenz und Dach für über 60 Standards
- Freiwillige Basis





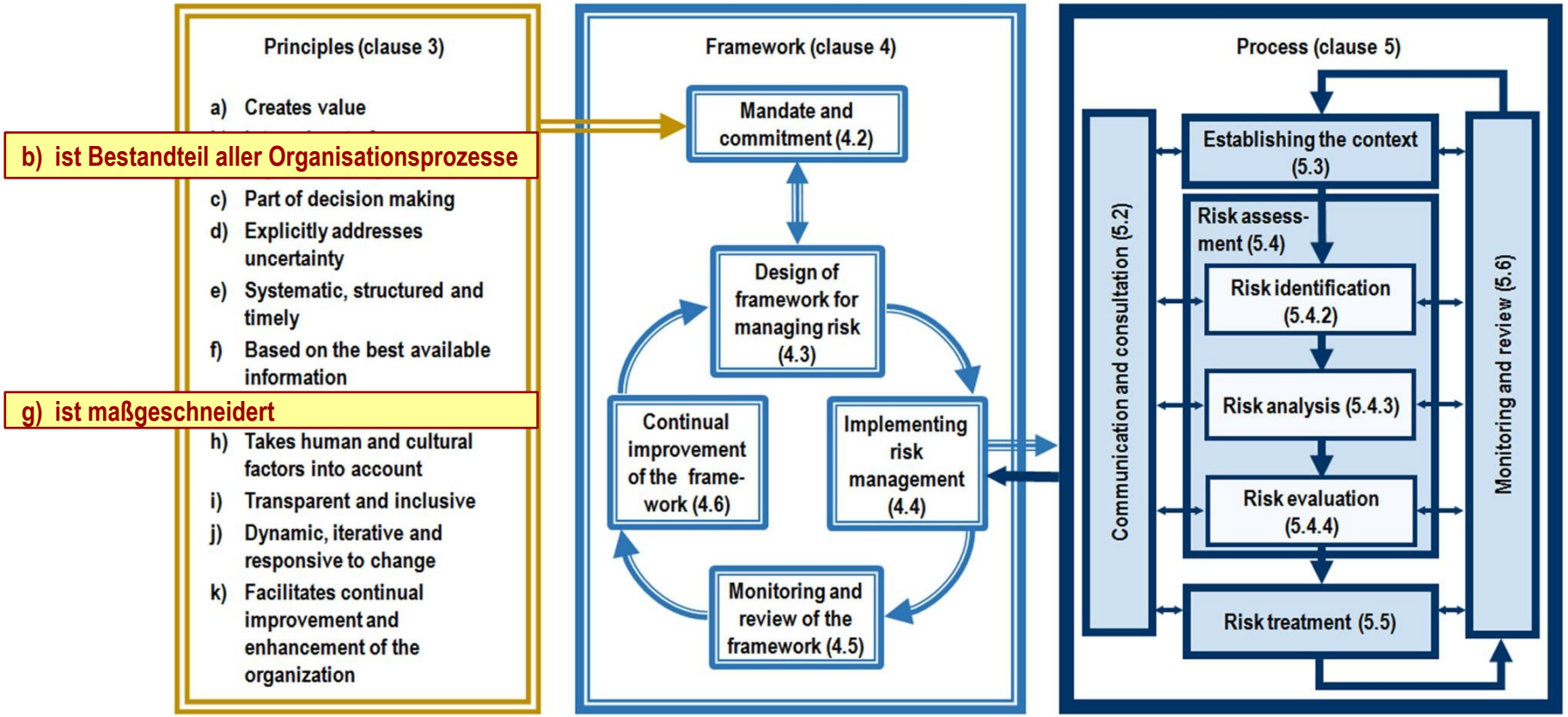
internationale Best Practice Regeln !

ISO 31000
Struktur (drei Säulen)



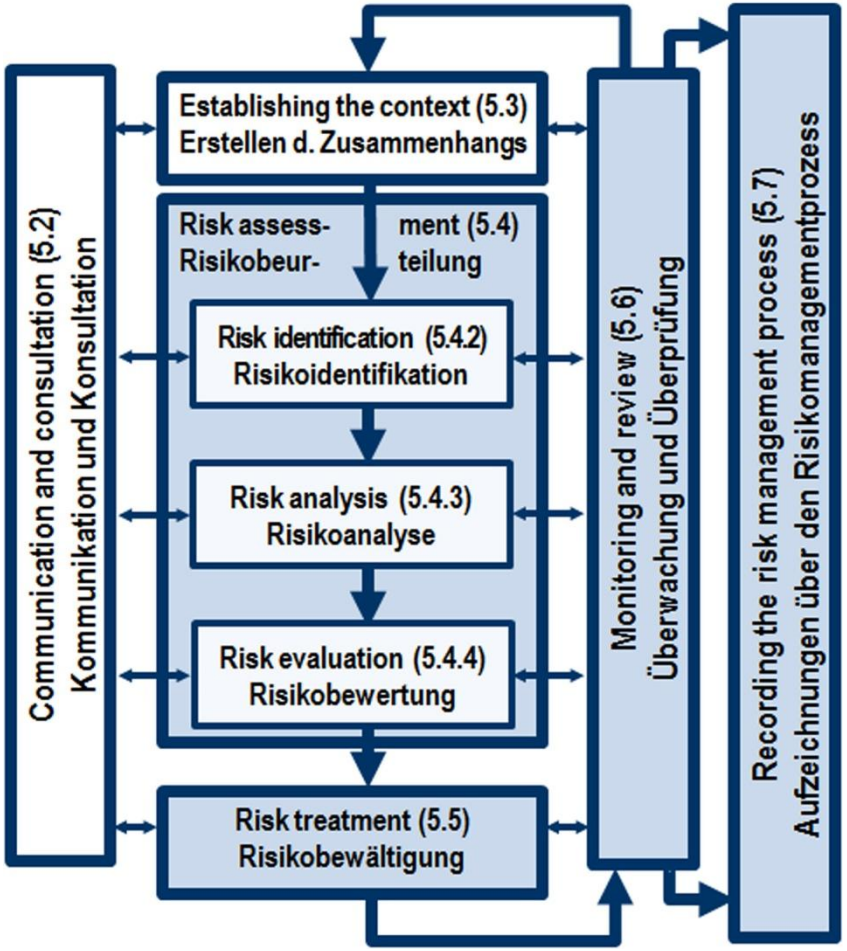
ISO 31000:2009 Einleitung, Bild 1

ISO 31000
Grundsätze



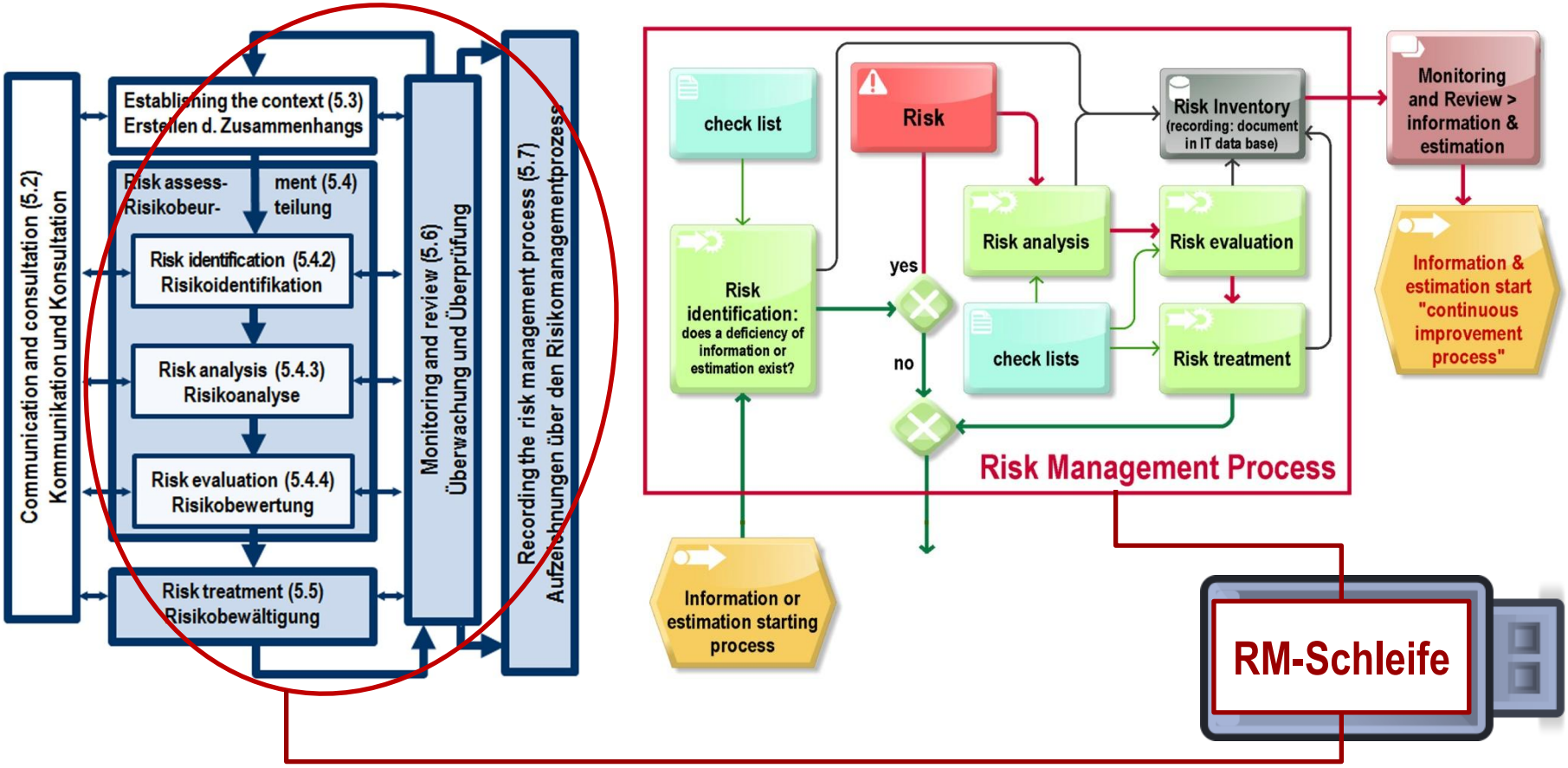
ISO 31000
Der Kernprozess

Kapitel 5.1: Der Risikomanagement-prozess sollte ein integrierter Teil des Managements sein



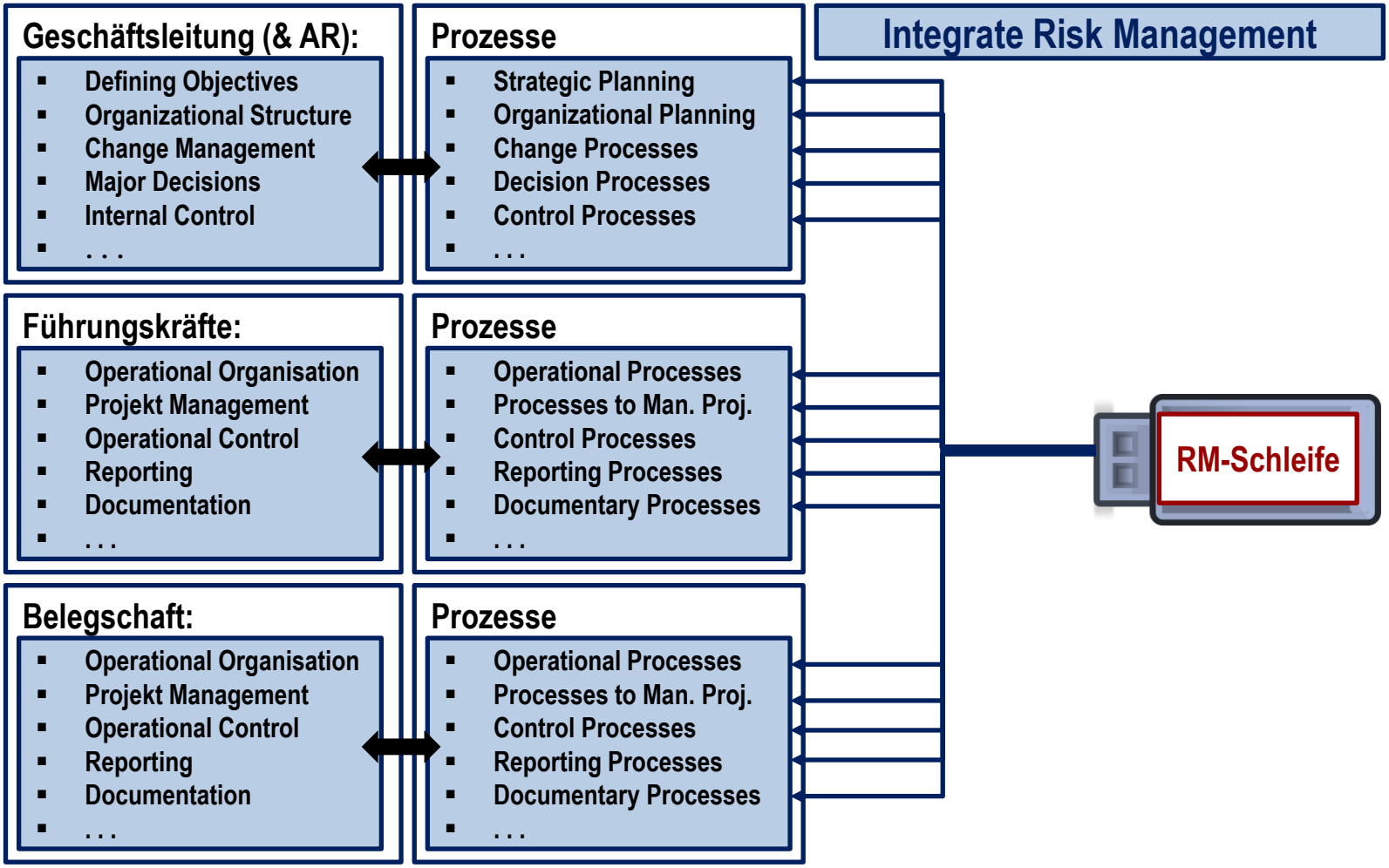
ISO 31000:2009 Abschnitt 5 Prozess, Bild 3 abgewandelt

Der Kernprozess
Die RM-Schleife als »Plug-in Dongle«

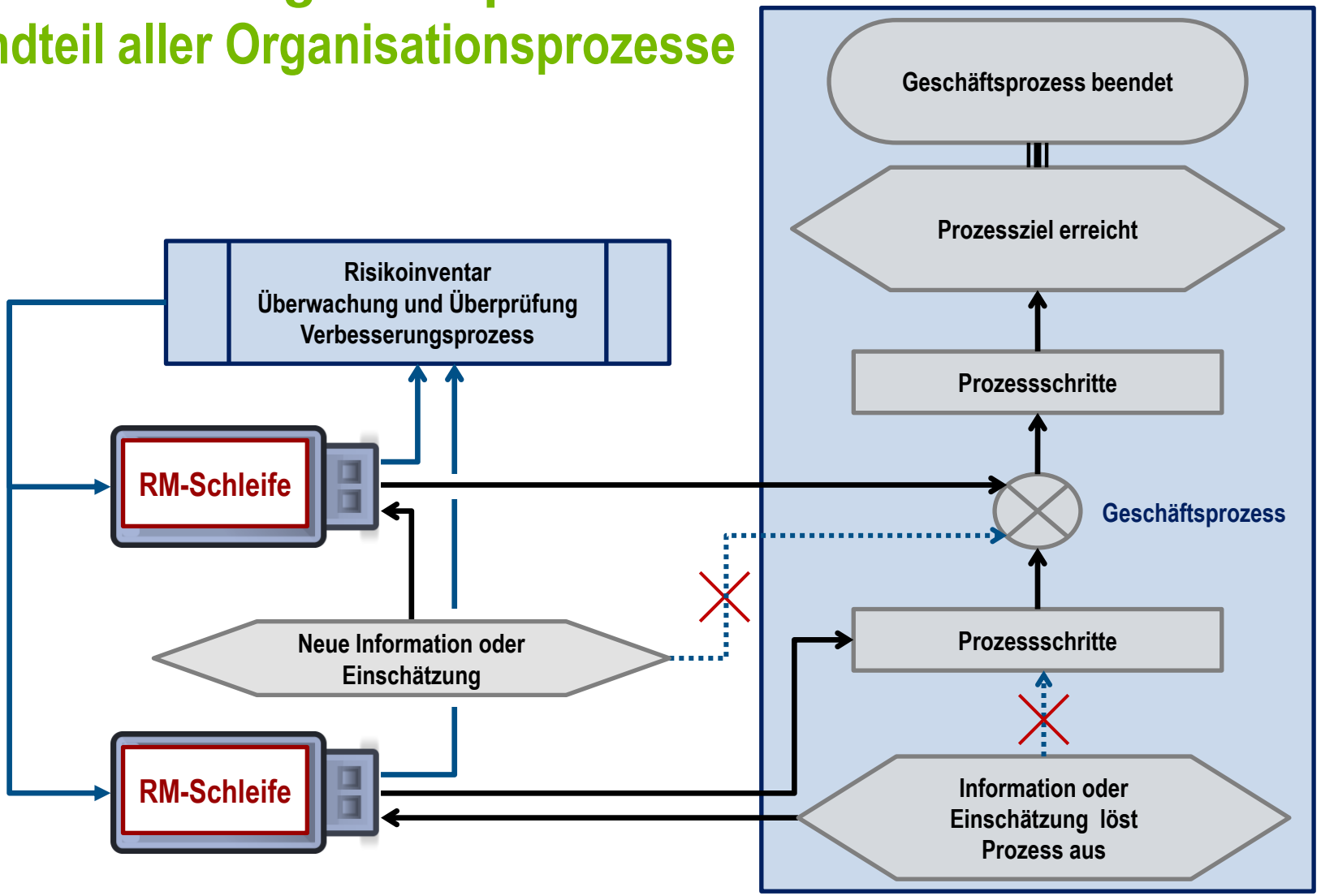


Der Risikomanagementprozess

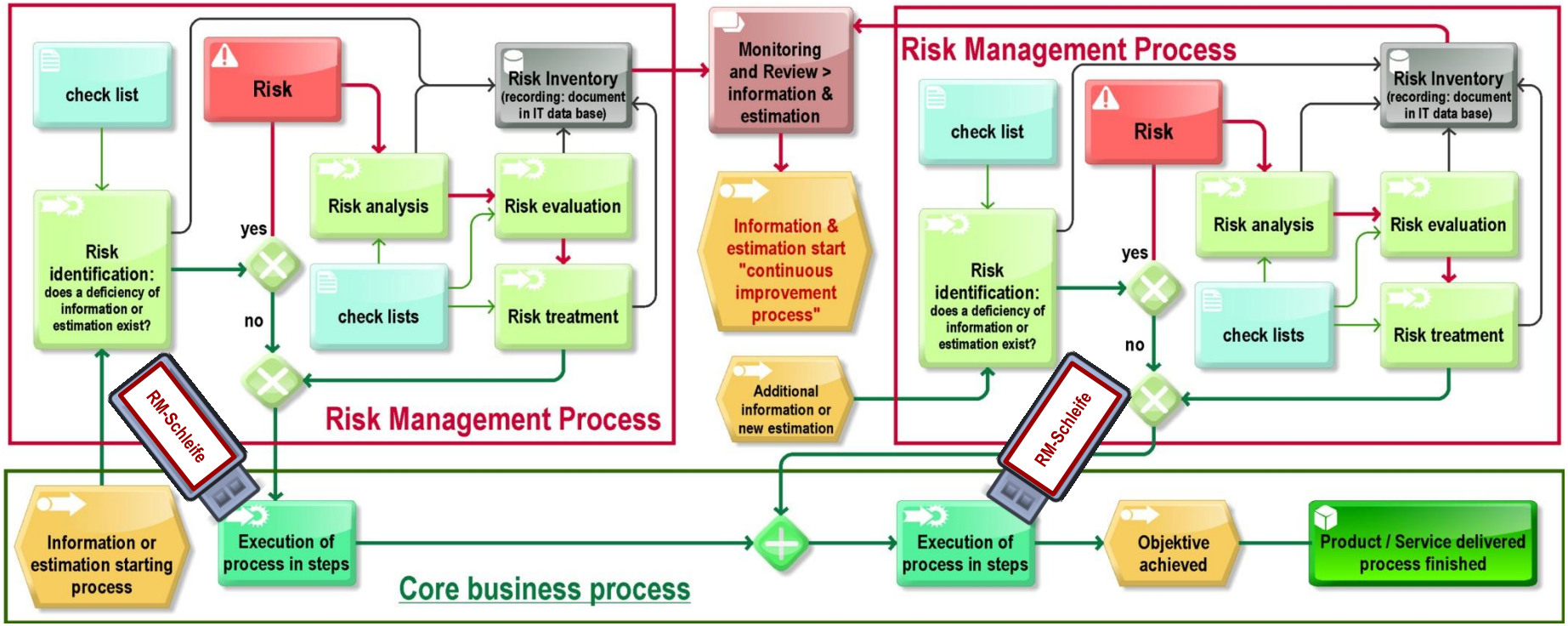
ist Bestandteil aller Organisationsprozesse



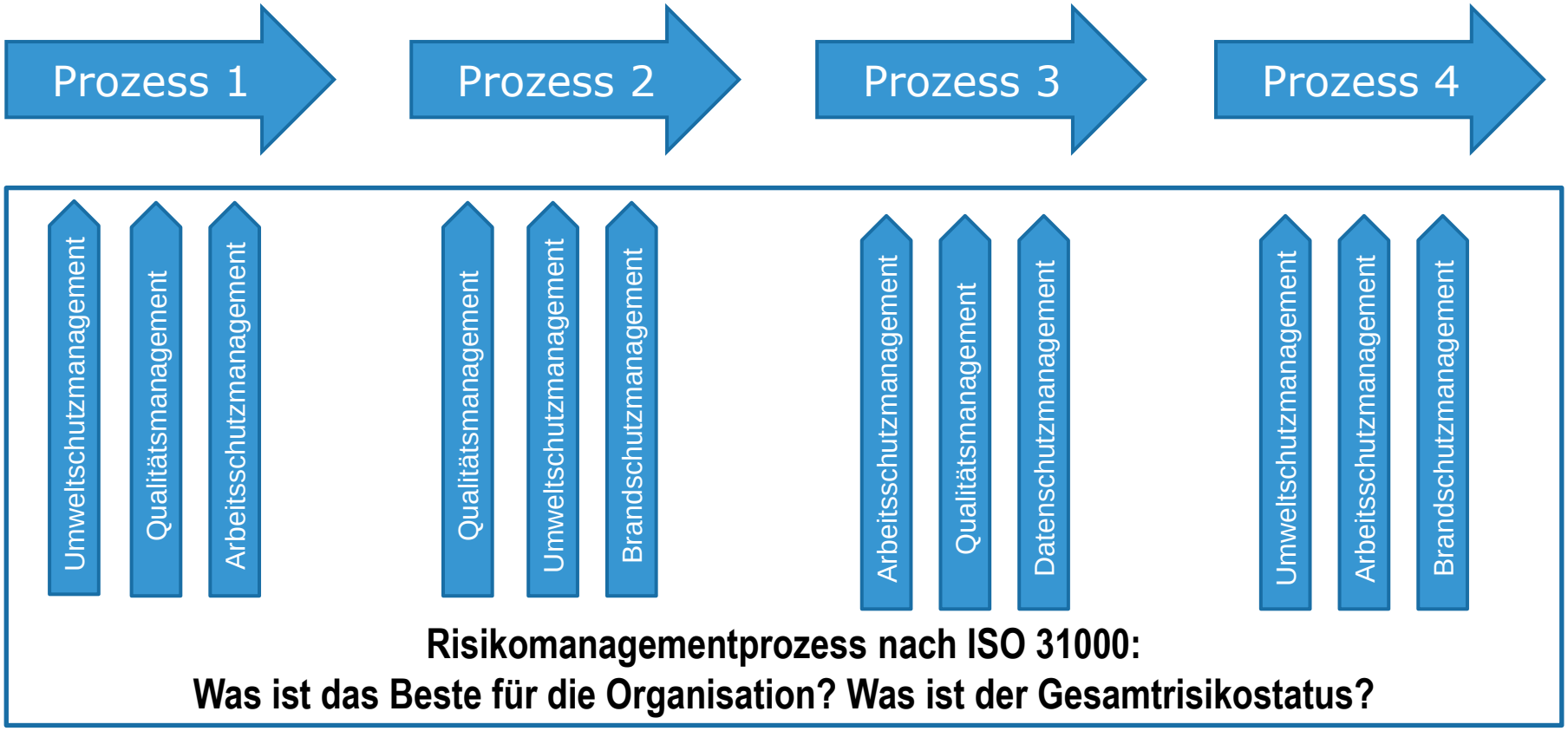
Der Risikomanagementprozess ist Bestandteil aller Organisationsprozesse



Der Risikomangementprozess als Bestandteil eines Organisationsprozesses



Klammerfunktion der ISO 31000
für bestehende Managementsysteme



(Grafik in Anlehnung an: Weis, Udo; Risikomanagement nach ISO 31000; WEKA 2012)

Managementsystemnormen der ISO
Annex SL Appendix 2

»High Level Structure«

- 2012 vom ISO (International Organization for Standardization) Lenkungsgremium eingeführt
- Festlegung in den ISO/IEC Directives, Part 1 Consolidated ISO Supplement – Procedures Specific to ISO – Annex SL, Appendix 2 (normative)
- Deutsche (D-A-CH) Fassung: DIN Spec 36601 (Beuth Verlag: http://www.beuth.de)

Einheitliche Grundstruktur für Managementsystemnormen (»MSS«)

- Einheitliche Gliederung, einheitlicher Basistext und Definitionen der wichtigsten Grundbegriffe
- Zwei Alternativen:
  (1) **Typ-A:** Anforderungen (**Requirements** – zertifizierbar)
  (2) **Typ-B:** Empfehlungen (**Recommendations/Guidelines** – nicht zertifizierbar)

Ziel

- Anwenderfreundlichkeit fördern und den Aufwand zur Umsetzung verschiedener Systeme reduzieren
- Integration der Managementsysteme einer Organisation ermöglichen/erleichtern
- Risikobasierter Ansatz (»risikobasiertes Denken«) ➡ **managing based on risk management**

HLS (High Level Structure)
ISO/IEC Directives Part 1 – Annex SL, Appendix 2

- **Einleitung**
- 1 **Anwendungsbereich** (Scope)
- 2 **Normative Verweisungen** (Normative references)
- 3 **Begriffe** (Terms and definitions)
- 4 **Kontext der Organisation** (Context of the Organisation)
- 5 **Führung** (Leadership)
- 6 **Planung** (planning)
- 7 **Ressourcen** (Ressources)

Plan

- 8 **Betrieb** (Operation

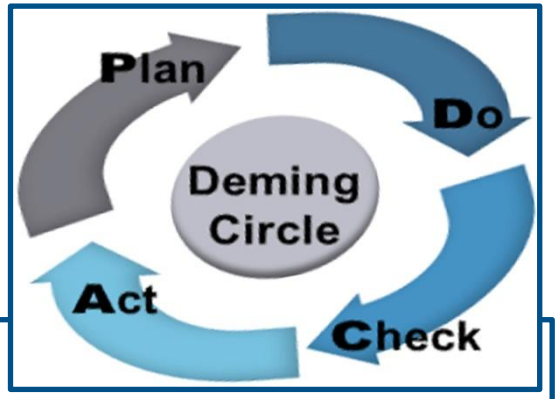
Do

- 9 **Bewertung der Leistung** (Performance evaluation)

Check

- 10 **Verbesserung** (Improvement)

Act



Risikobasierter Ansatz
6 Planung (DIN Spec 36601)

6.1 Maßnahmen zum Umgang mit Risiken und Chancen

Bei Planungen für das [*XXX*]managementsystem muss die Organisation die in 4.1 genannten Themen und die in 4.2 genannten Anforderungen berücksichtigen **sowie die Risiken und Chancen bestimmen, die betrachtet werden müssen, um**

- sicherzustellen, dass das [*XXX*]managementsystem seine beabsichtigten Ergebnisse erzielen kann,
- unerwünschte Auswirkungen zu verhindern oder zu verringern,
- fortlaufende Verbesserung zu erreichen.

Die Organisation muss planen:

a) Maßnahmen zum Umgang mit diesen Risiken und Chancen;

b) wie
- die Maßnahmen in die [*XXX*]managementsystem-Prozesse der Organisation integriert und dort umgesetzt werden;
- die Wirksamkeit dieser Maßnahmen bewertet wird.

Risikobasierter Ansatz
8 Betrieb (DIN Spec 36601)

8.1 Betriebliche Planung und Steuerung

Die Organisation muss die Prozesse zur Erfüllung der Anforderungen und zur Durchführung der **unter 6.1 bestimmten Maßnahmen** planen, verwirklichen und steuern, indem sie:

- Kriterien für die Prozesse festlegt;
- die Steuerung der Prozesse in Übereinstimmung mit den Kriterien durchführt;
- dokumentierte Information im notwendigen Umfang bereithält, so dass darauf vertraut werden kann, dass die Prozesse wie geplant durchgeführt wurden.

Die Organisation muss geplante Änderungen überwachen sowie die Folgen unbeabsichtigter Änderungen beurteilen und, falls notwendig, Maßnahmen ergreifen, um jegliche negativen Auswirkungen zu vermindern.

Die Organisation muss sicherstellen, dass ausgegliederte Prozesse gesteuert werden.

Risikobasierter Ansatz
ISO 19600 *Compliance management systems - Guidelines*

6.1 Actions to address compliance risks

When planning for the compliance management system, the organization should consider the issues referred to in **4.1 [*Verstehen der Organisation und ihres Kontextes*]**, the requirements referred to **in 4.2 [*Verstehen der Erfordernisse und Erwartungen interessierter Parteien*]**, the principles of good governance referred to in **4.4 [*Compliance Management System und Prinzipien guter Führung*]**, the compliance obligations identified in **4.5 [Compliance Pflichten]** **and the results of the compliance risk assessment referred to in 4.6 [*Identifikation, Analyse und Bewertung von Compliance Risiken*]*** to determine the compliance risks that need to be addressed to:

– assure the compliance management system can achieve its intended outcome(s);
– prevent, detect and reduce undesired effects;
– achieve continual improvement.

The organization should plan:

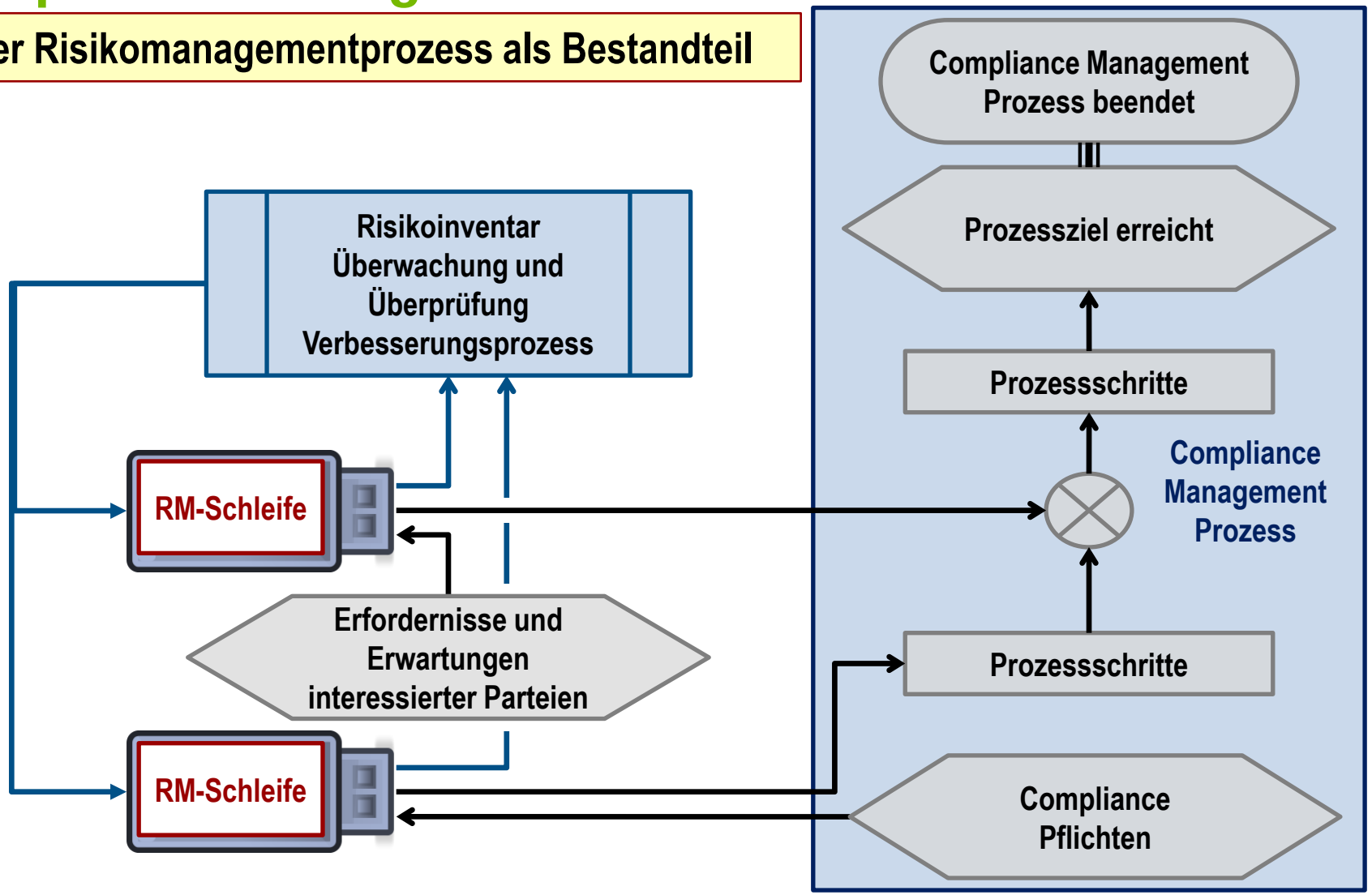
a) actions to address these compliance risks and
b) how to:
   – integrate and implement the actions into its compliance management system processes;
   – evaluate the effectiveness of these actions.

The organization should retain documented information on the compliance risks and on the planned actions to address them.

*** In NOTE 1 und NOTE 2: »Risk based approach« & Verweis auf ISO 31000**

Compliance Management Prozess

der Risikomanagementprozess als Bestandteil



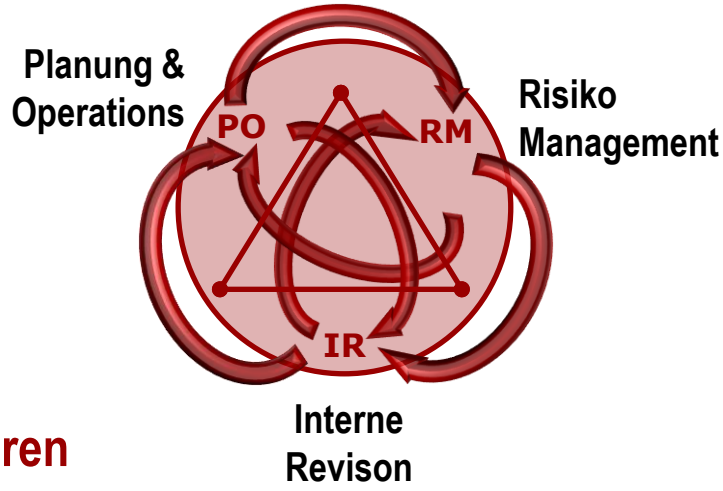
Anhang:
Abgleich mit der Internen Revision

Die laufende oder zumindest periodische Aktualisierung des Risikoinventars und der Überprüfung der Kontrollaktivitäten werden einerseits

- ☛ von der Internen Revision überprüft

und die Ergebnisse bilden andererseits

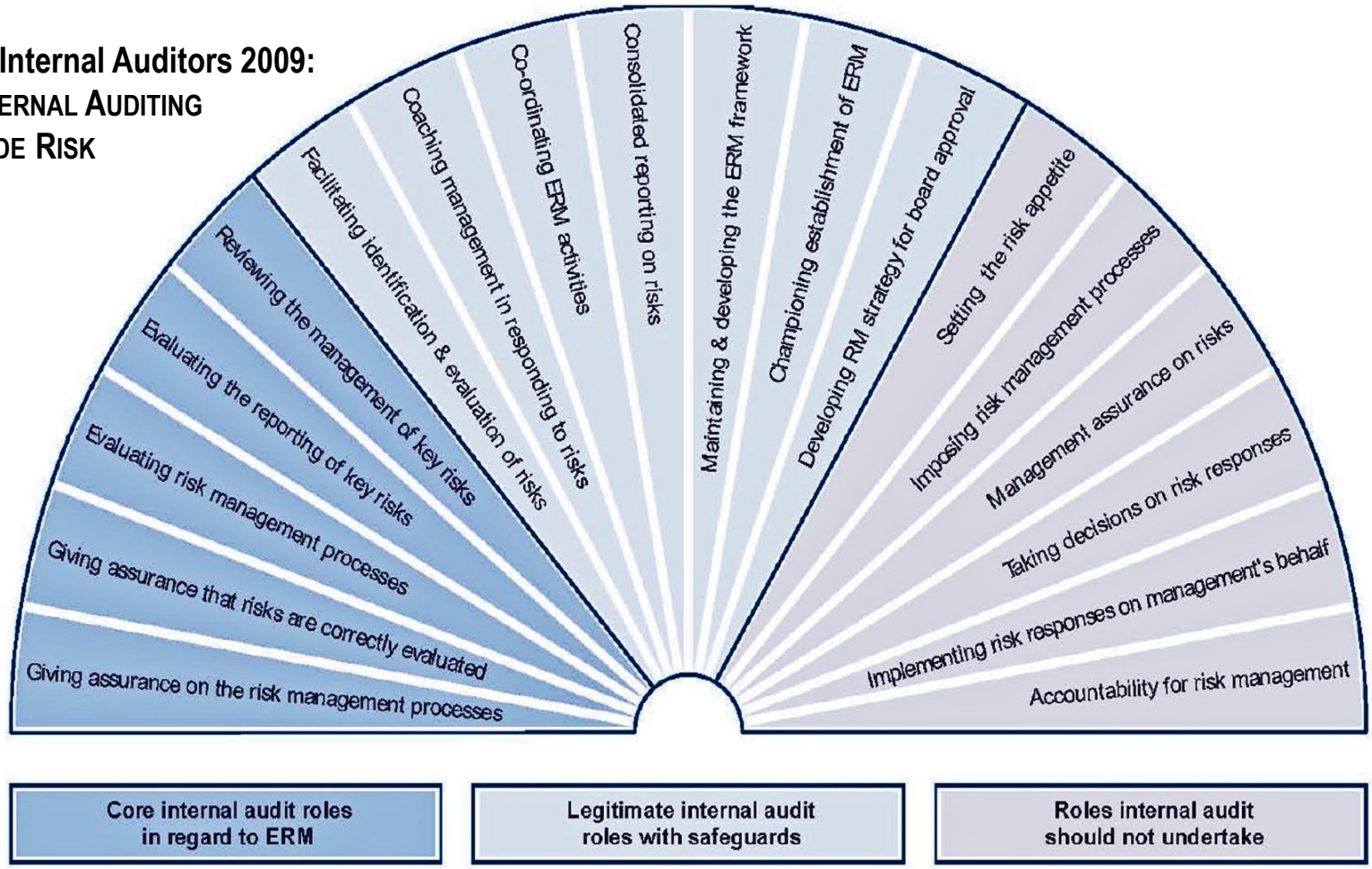
- ☛ die Basis für die Jahresplanung der internen Revision



➡ Die interne Revison findet auf einem höheren Reifegrad mit einem qualitativen anstelle eines quantitativen Ansatzes statt.

Die Interne Revision im Risikomanagement

The Institute of Internal Auditors 2009:
THE ROLE OF INTERNAL AUDITING IN ENTERPRIZEWIDE RISK MANAGMENENT



https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Role%20of%20Internal%20Auditing%20in%20Enterprise%20Risk%20Management.pdf

Vielen Dank Für Ihre Aufmerksamkeit!

© & Kontakt:

DR. FRANK HERDMANN RECHTSANWALT
AUXILIUM MANAGEMENT SERVICE

Gluckweg 10 | 12247 Berlin | Germany
Phone: +49 30 - 771 90 321
Fax: +49 30 - 771 90 322
Mobile: +49 172 - 301 90 24
Email: auxilium@herdmann.de

ISO Head of ISO/TC 262 AG 1 *Communications*

DIN NA 175-00-04 *Risikomanagement* , stellvertretender Obmann