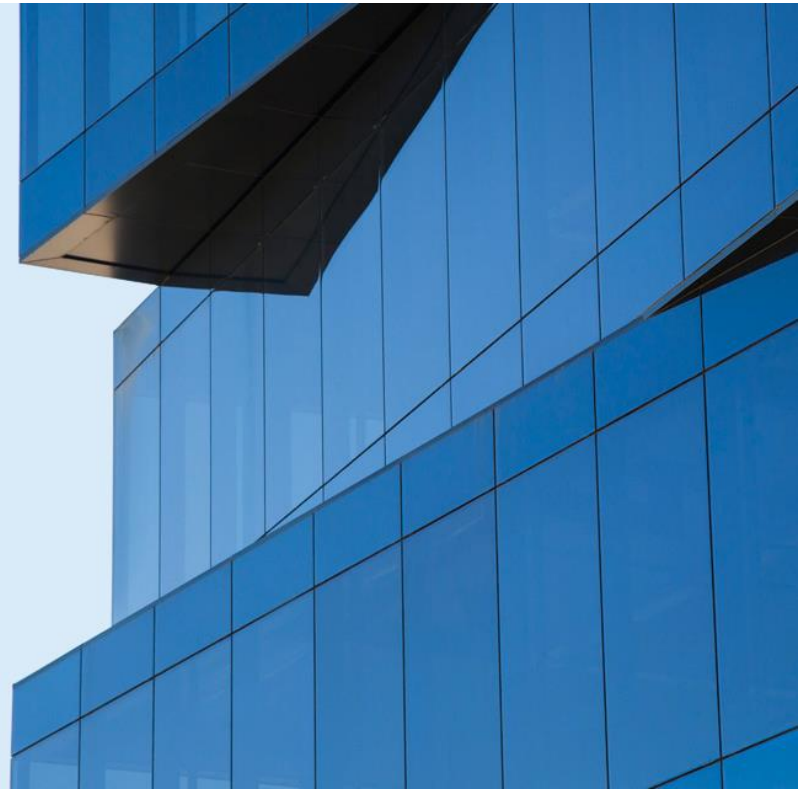


Dr. Frank Herdmann
22.08.2019

Kurze Einführung in effektives und effizientes Risikomanagement nach DIN ISO 31000



Einführung und Grundlagen

Gliederung

- Was ist Risiko?
- Was ist Risikomanagement und warum ist es sinnvoll?
- DIN ISO 31000 und konkurrierende Regelungen
- DIN ISO 31000, ihre Struktur und ihr Inhalt
 - Grundsätze
 - Rahmenwerk
 - Prozess



Was ist Risiko?

Risikodefinitionen (keine erschöpfende Auflistung)

- The possibility that events will occur and affect the achievement of strategy and business objectives (COSO)
- Combination of the occurrence of harm and the severity of that harm (ISO Guide 51:2014 & e.a.)
- **Auswirkung von Unsicherheit auf Ziele** (effect of uncertainty on objectives) – **DIN ISO 31000:2018 e.a.**
- effect of uncertainty ISO 9000:2015 e.a.

IWA 31 (Entwurf 19. August 2019):

- »An objective can be expressed as an intended outcome or result.«
- »A combination of the occurrence of harm and the severity of harm can be considered to be included in the broader definition of risk in 3.1 of ISO 31000«



Was ist Risikomanagement und warum ist es sinnvoll?

Die Menschheit ist über die Zeiten erfolgreich gewesen und hat überlebt, weil sie die Fähigkeit zum Umgang mit Risiken erworben hat: die Entscheidung zu treffen, wegzulaufen oder den Angreifer zu bekämpfen, ist Risikomanagement!

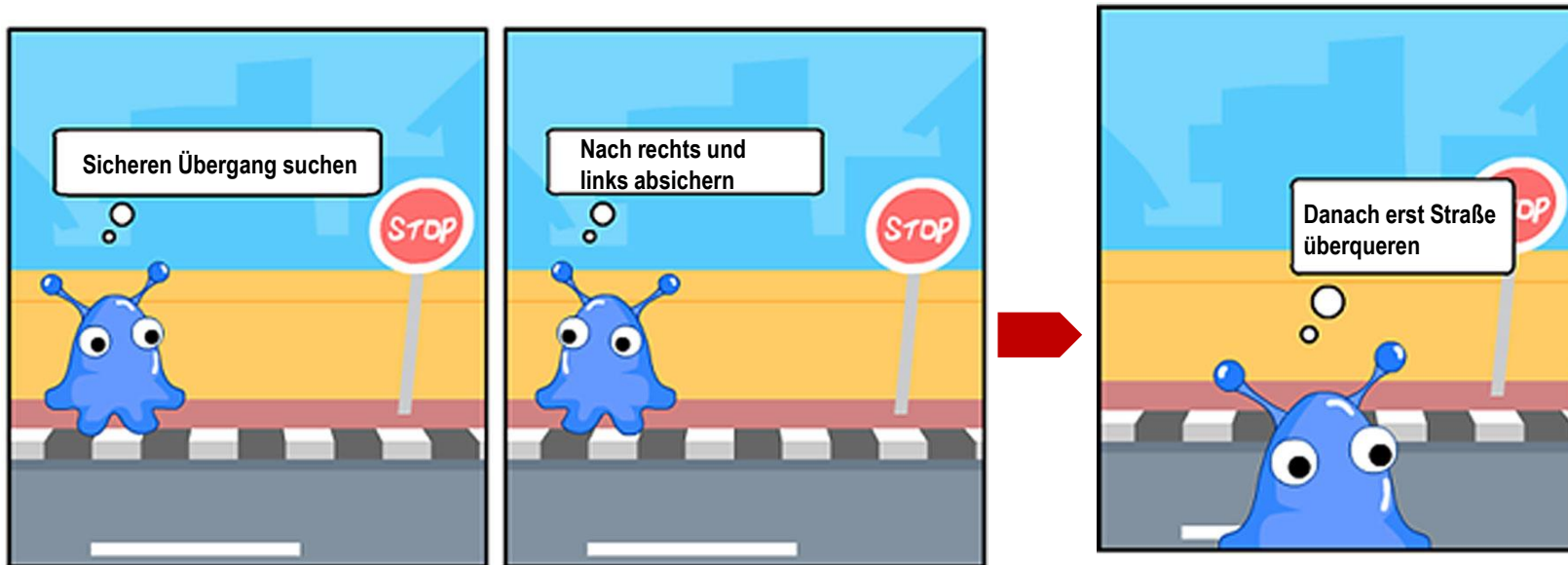


"Dieses Foto" von Unbekannter Autor ist lizenziert gemäß CC BY-NC

Risikomanagement in seinen ersten Schritten ist eine einfache Aufgabe, die gesunden Menschenverstand verlangt – was jeder Manager beachten sollte, der seine Pflicht, seine Organisation widerstandsfähig zu erhalten, ernst nimmt.

Was ist Risikomanagement und warum ist es sinnvoll?

Wichtige Fragen



Effektives und effizientes Risikomanagement nach DIN ISO 31000

Nationale Regeln

Rechtlicher Kontext in Deutschland:

- KonTraG seit 1. Mai 1998 in Kraft
- Bilanzrechtsreformgesetz (BilReG):
- Bilanzrechtsmodernisierungsgesetz (BilMoG) vom Mai 2009:
- Kreditwesengesetz (KWG):

Nationale Prüfnormen in Deutschland (Institut der Wirtschaftsprüfer in Deutschland e.V.):

- IDW PS 340 (Prüfung des Risikofrüherkennungssystem – letzte Auflage 2000)
- IDW PS 981 (Prüfung von Risikomanagementsystemen – März 2017)

Internationale Normen

Beispiele:

- **AS NZS 4360:1995 Risk Management Standard**, Australien & Neuseeland 1995 (inzwischen ersetzt durch AS ISO 31000: 2018 Risk Management - Guidelines)
- **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 – ersetzt durch Enterprise Risk Management – Integrating Strategy and performance im Juni 2017)
- **ONR 49000:2004 ff. Risikomanagement für Organisationen und Systeme: Begriffe und Grundlagen** (Österreich 2004 – in Überarbeitung)
- **ISO 31000:2009 Risk Management – Principles and guidelines** (international, 2009 – ersetzt durch ISO 31000:2018 Risk management – Guidelines im Februar 2018)

DIN ISO 31000 und ihre Struktur

Drei Säulen:

- **Grundsätze:** erforderliche Eigenschaften eines wirksamen und effizienten Risikomanagements
- **Rahmenwerk:** Hilft bei der Integration des Risikomanagements in die Aktivitäten und Funktionen der Organisation
- **Prozess:** integraler Bestandteil von Management, Struktur, Abläufen und Prozessen der Organisation

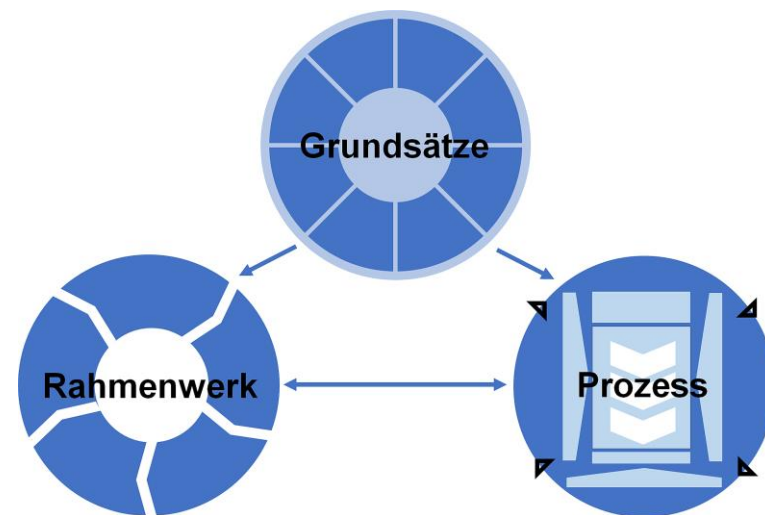


Bild 1 – Grundsätze, Rahmenwerk und Prozess (vereinfacht)

Der Inhalt der DIN ISO 31000:2018

Die Grundsätze

Kernkonzept der DIN ISO 31000: Der Zweck des Risikomanagements besteht in der Schaffung und dem Schutz von Werten.

- **Acht Grundsätze** (Konzepte) vermitteln den Wert des Risikomanagements, erläutern Absicht und Zweck und bilden die Grundlage für das Umgehen mit Risiken rund um die Schaffung und den Schutz von Werten.
- **Die Grundsätze sind erforderlich für ein effektives und effizientes Risikomanagement**

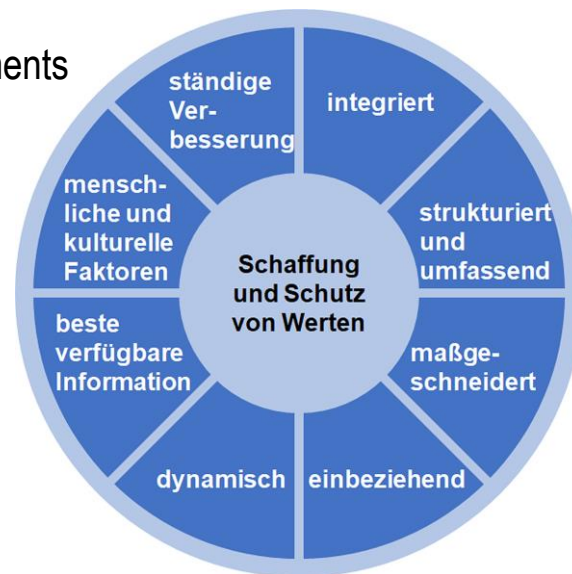


Bild 2 – Grundsätze

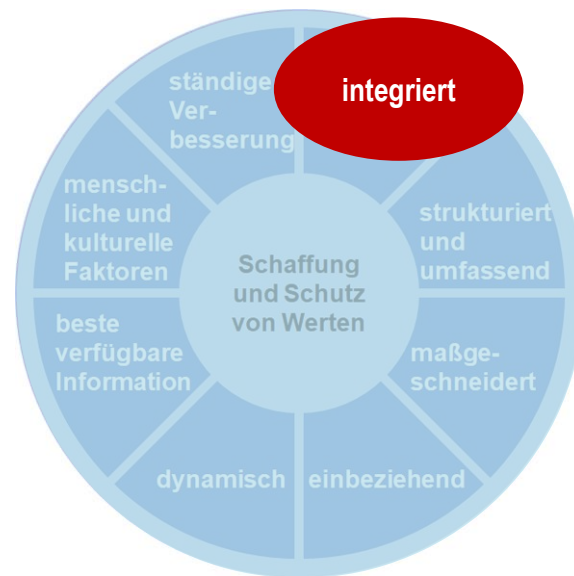
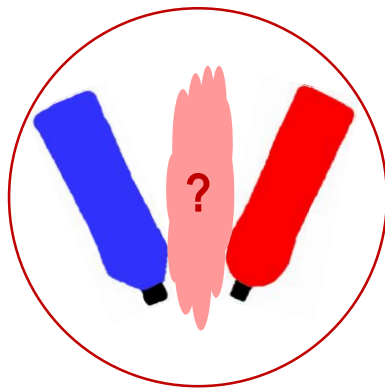
Der Inhalt der DIN ISO 31000:2018

Die Grundsätze

- a) integriert

Risikomanagement ist ein integraler Bestandteil aller Aktivitäten einer Organisation.

z.B. die Reinigungskraft →



Der Inhalt der DIN ISO 31000:2018

Die Grundsätze

- c) maßgeschneidert

Das Rahmenwerk und die Prozesse des Risikomanagements sind an den externen und internen Kontext einer Organisation angepasst und diesem angemessen sowie mit den Zielen der Organisation verbunden.

Vergleiche Abschnitt 5.1 (Rahmenwerk): Die Komponenten des . . . und die Art und Weise, in der diese ineinandergreifen, sollten an die Bedürfnisse der Organisation angepasst werden.



Der Inhalt der DIN ISO 31000:2018

Das Rahmenwerk

- Abschnitt 5 der Norm beschreibt in 7 Kapiteln die Elemente des Rahmenwerkes, die der Organisation die Integration von Risikomanagement in Ihre Aktivitäten und Funktionen erleichtern sollen.
- **Bild 3 der Norm zeigt die Komponenten des Rahmenwerks**
- Die Komponenten sollen an die Bedürfnisse der Organisation (**maßgeschneidert**) angepasst werden



Bild 3 – Rahmenwerk

Der Inhalt der DIN ISO 31000:2018

Das Rahmenwerk – Abschnitt 5.2

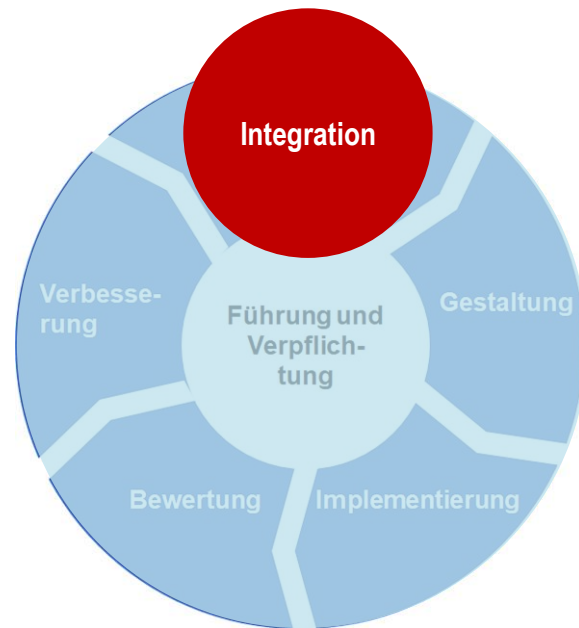
- **Führung und Verpflichtung (oberste Leitung und, wo angezeigt, die Aufsichtsorgane)**
 - Anpassen und Implementieren der Komponenten des Rahmenwerks
 - Veröffentlichen eines Grundsatzdokuments
 - Bereitstellung der erforderlichen Ressourcen
 - Zuweisen von Befugnis, Verantwortlichkeit und Rechenschaftspflicht



Der Inhalt der DIN ISO 31000:2018

Das Rahmenwerk – Abschnitt 5.3

- **Integration (► ◄ Silo-Aktivität)**
 - Jeder in der Organisation ist verantwortlich für den Umgang mit Risiken
 - Dynamischer und iterativer Prozess angepasst an die Bedürfnisse und die Kultur der Organisation
 - Bereitstellung der erforderlichen Ressourcen
 - Zuweisen von Befugnis, Verantwortlichkeit und Rechenschaftspflicht



Der Inhalt der DIN ISO 31000:2018

Das Rahmenwerk – Abschnitt 5.4

■ Gestaltung

- Verstehen der Organisation und ihres Zusammenhangs
- Artikulieren der Risikomanagementverpflichtung
- Zuweisen von organisatorischen Rollen, Befugnissen, Verantwortlichkeiten und Rechenschaftspflichten
- Zuordnung von Ressourcen
- Einrichten der Kommunikation und Konsultation



Der Inhalt der DIN ISO 31000:2018

Der Prozess

- Der Risikomanagementprozess soll integraler Bestandteil des Managements und der Entscheidungsfindung der Organisation sein
- Er soll in die Struktur , die Abläufe und Prozesse (alle Aktivitäten) integriert und auf allen Ebenen angewendet werden.
- Es können viele (unterschiedliche) Anwendungen des Prozesses innerhalb einer Organisation bestehen, an die er jeweils (maßgeschneidert) anzupassen ist.
- Zumeist sequentiell dargestellt, ist er tatsächlich iterativ

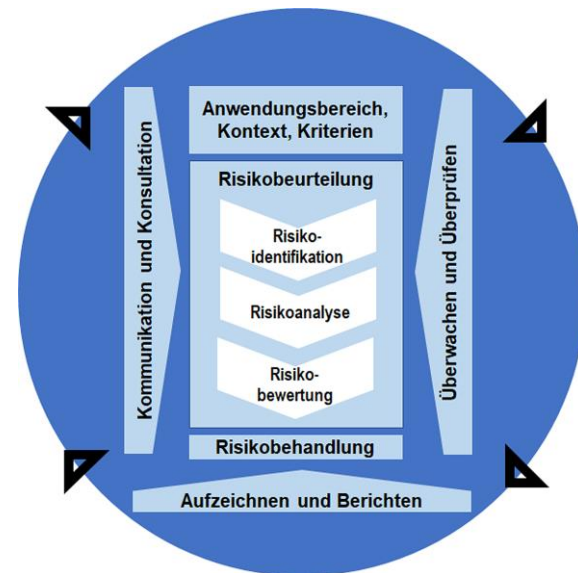


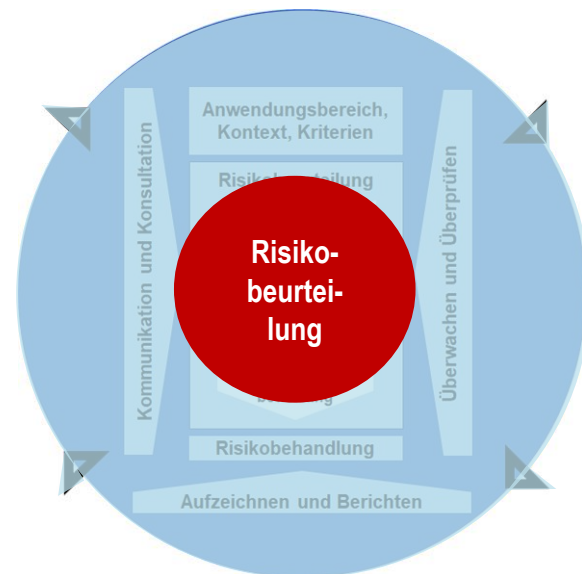
Bild 4 – Prozess

Der Inhalt der DIN ISO 31000:2018

Der Prozess – Abschnitt 6.4

■ Risikobeurteilung

- Sollte systematisch, iterativ und kollaborativ durchgeführt werden
- Hilfsmittel für die Risikobeurteilung finden sich in der ISO/IEC 31010
- Risikobeurteilung ist der Prozess der
 - Risikoidentifikation
 - Risikoanalyse und der
 - Risikobewertung



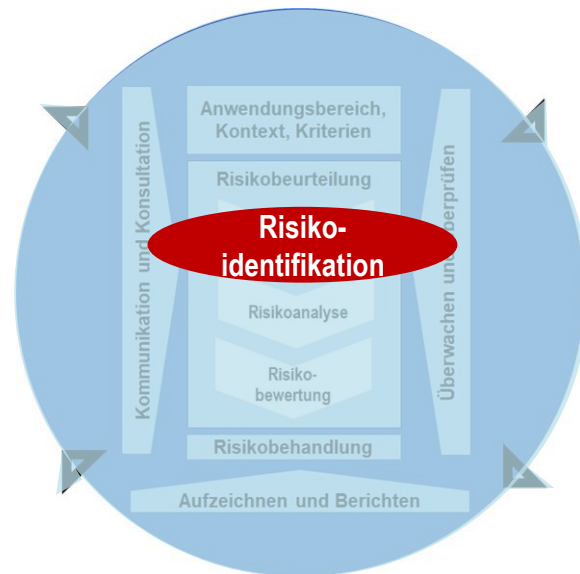
Der Inhalt der DIN ISO 31000:2018

Der Prozess – Abschnitt 6.4.2

■ Risikoidentifikation

- Finden, erkennen und beschreiben von Risiken, die einer Organisation helfen oder sie daran hindern können, ihre Ziele zu erreichen.
- Die Verfügbarkeit relevanter geeigneter und aktueller Informationen ist für das Identifizieren von Risiken wichtig.
- Ein nicht identifiziertes Risiko wird weder analysiert noch bewertet – noch kann es behandelt werden

Das größte Risiko aller Risiken besteht darin, die Risiken für die eigenen Ziele nicht zu berücksichtigen!



Der Inhalt der DIN ISO 31000:2018

Der Prozess – Abschnitt 6.4.3

■ Risikoanalyse

- Ziel ist es, die Art des Risikos, dessen Eigenschaften und gegebenenfalls die Risikohöhe zu verstehen.
- Sie umfasst eine ausführliche Betrachtung von Unsicherheiten, Risikoursachen, Auswirkungen, Wahrscheinlichkeit etc.
- Sie kann mit unterschiedlichem Detailierungsgrad und Komplexität je nach Zweck und Ressourcen durchgeführt werden.
- Analysetechniken können qualitativ, quantitativ oder eine Kombination davon sein.



Der Inhalt der DIN ISO 31000:2018

Der Prozess – Abschnitt 6.4.4

■ Risikobewertung

- Der Zweck ist es, Entscheidungen zu unterstützen.
- Sie beinhaltet den Vergleich der Ergebnisse der Risikoanalyse mit den festgelegten Risikokriterien zur Feststellung, wo zusätzliche Aktionen erforderlich sind. Das kann zu Entscheidungen führen:
 - nichts weiter zu unternehmen;
 - Optionen zur Risikobehandlung zu erwägen;
 - weitere Analysen durchzuführen;
 - bestehende Steuerungen aufrechtzuerhalten;
 - Ziele zu überdenken.

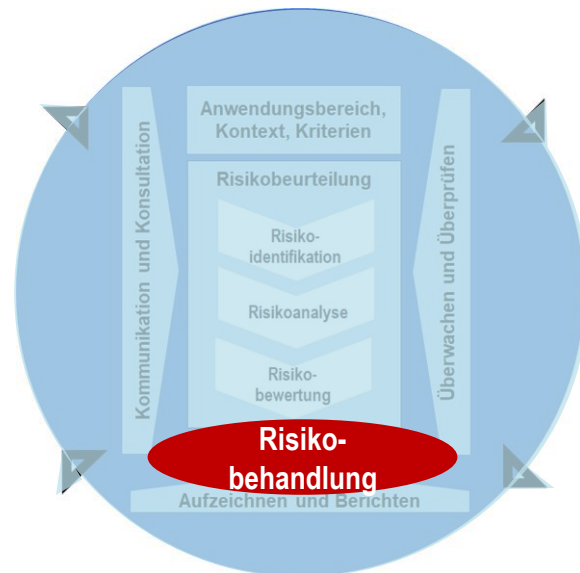


Der Inhalt der DIN ISO 31000:2018

Der Prozess – Abschnitt 6.5

■ Risikobehandlung

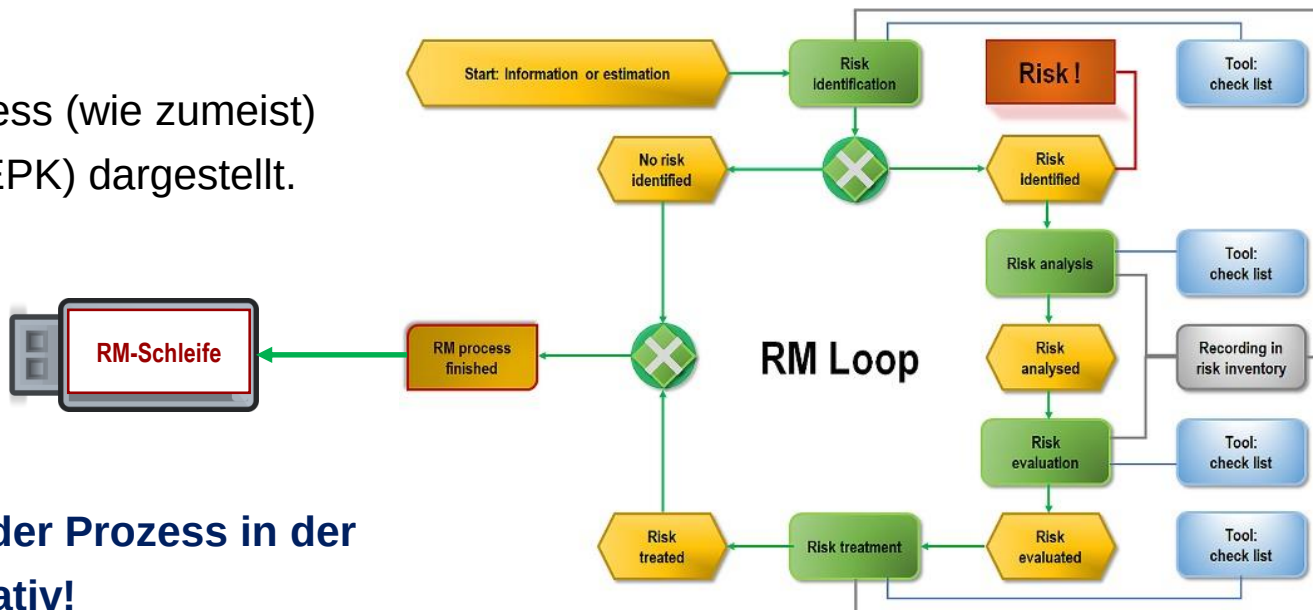
- Zweck ist es, Optionen zur Behandlung des Risikos auszuwählen und zu implementieren:
 - Auswahl von Optionen zur Behandlung des Risikos (Abwägung der erzielbaren Vorteile gegen die Kosten, den Aufwand oder die Nachteile – aber mehr als rein wirtschaftliche Erwägungen)
 - Erstellen und Implementieren von Plänen zur Risikobehandlung
- Keine Optionen verfügbar ➡ Risiko dokumentieren und laufend überprüfen.



Integration

Die Risikomanagementschleife (der Kernprozess)

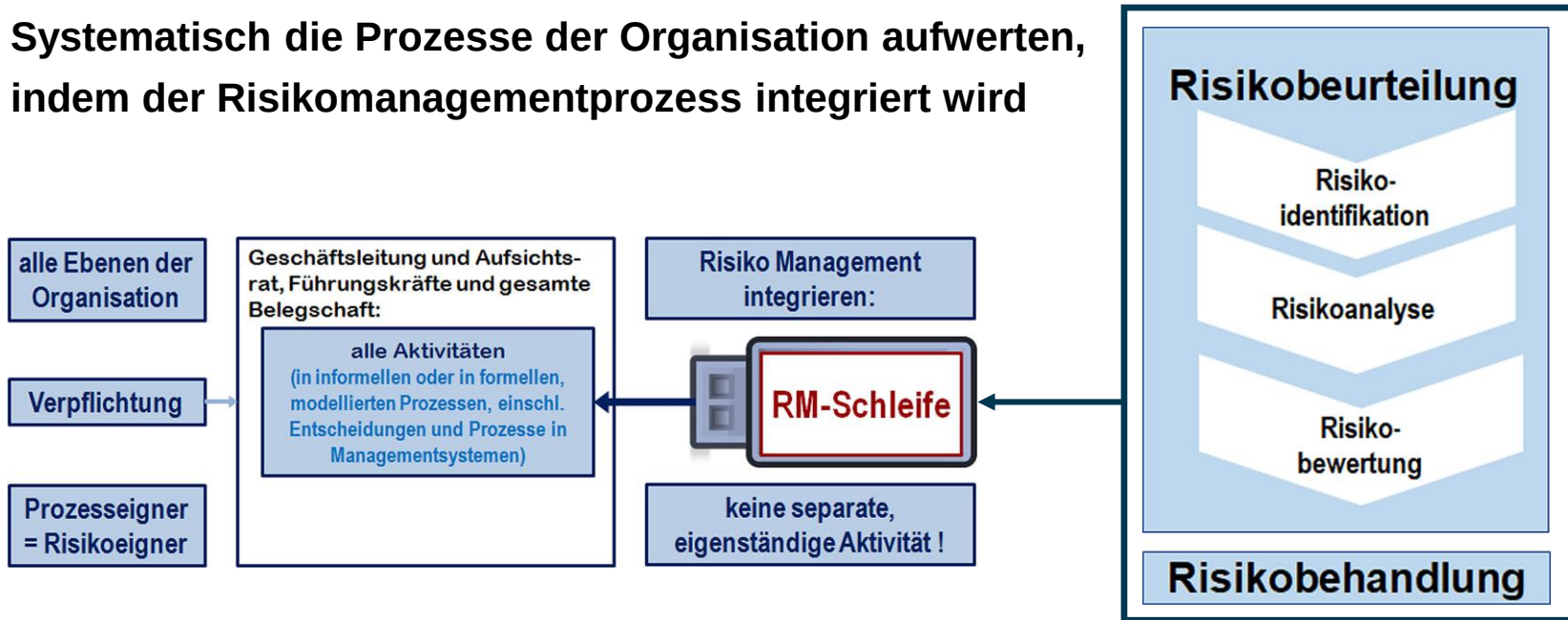
Hier ist der Prozess (wie zumeist) sequentiell (als EPK) dargestellt.



Tatsächlich ist der Prozess in der Praxis aber iterativ!

Integration

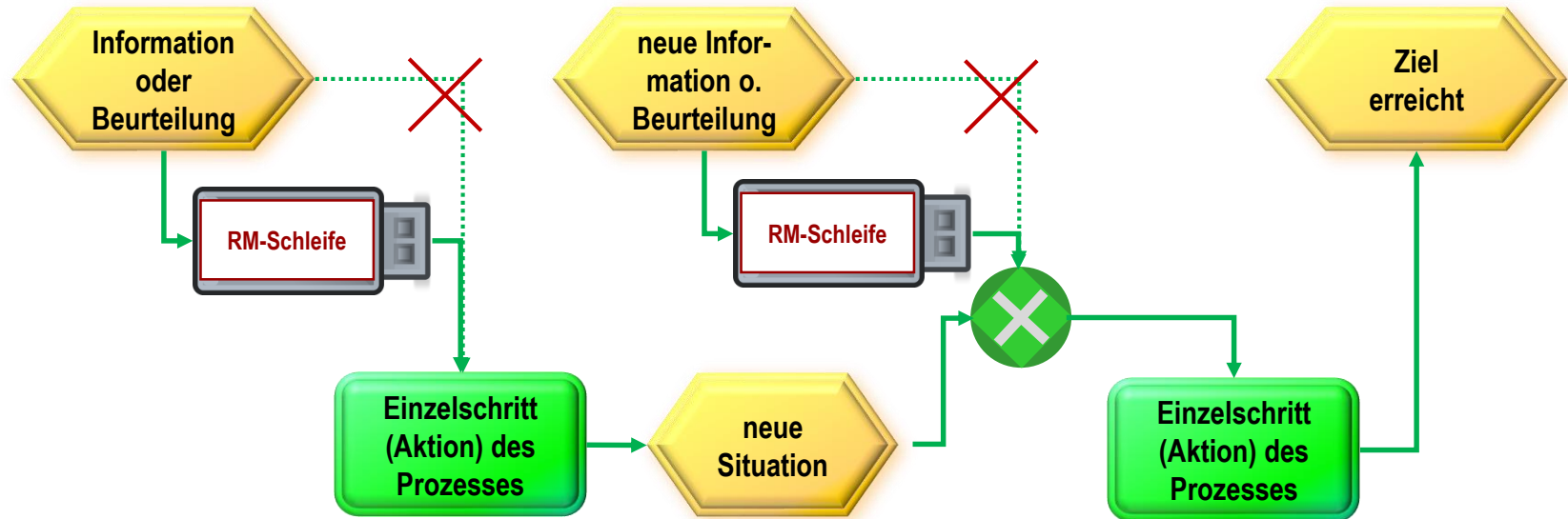
Systematisch die Prozesse der Organisation aufwerten, indem der Risikomanagementprozess integriert wird



Effektives und effizientes Risikomanagement nach DIN ISO 31000

Integration

Integration von Risikomanagement in einen operativen Prozess:



Vielen Dank für Ihre Aufmerksamkeit!

Sie haben noch Fragen? Sprechen Sie uns einfach direkt an.

Vorankündigung:

Seminar

**Effektives und effizientes Risikomanagement
Nach DIN ISO 3000 – Voraussetzung für gute
und verantwortungsvolle Unternehmensführung**

Termin: 22. Oktober 2019

DIN Akademie



Referent

A stylized blue logo consisting of a circle and a vertical line.

DR. FRANK HERDMANN RECHTSANWALT
AUXILIUM MANAGEMENT SERVICE
Managing Partner

Telefon 030 2601-0 (DIN-Akademie)
Mobil +49 172 3019 124 (Referent)
Telefax +49 30 771 90 322 (Referent)
auxilium@herdmann.de
www.herdmann.de
www.expatbiz.eu

