DIIR Deutsches Institut für Interne Revision e.V.

RMA RiskManagement Association e.V.

IT-Tagung 2016

Verzahnung von Information und Enterprise Risk Management – ISO 31000 in der IT

Ralf Kimpel, CIA, CRMA, Hubert Burda Media Holding KG
Michael Schmid, CISM, Hubert Burda Media Holding KG

Agenda

- **Risk Management Association e.V. (RMA) – die unabhängige Interessenvertretung von Enterprise Risk Managern im deutschsprachigen Raum**
- **Bedeutung und Entwicklung von COSO ERM, ISO 31000 und anderen relevanten Standards im Risikomanagement**
- **Zusammenarbeit von RMA und ISACA im Arbeitskreis „IT-Risikomanagement“**
- **Gemeinsamer ISACA-/RMA-Leitfaden zur ISO 31000 in der IT**

Risk Management Association e.V. (RMA) – die unabhängige Interessenvertretung von Enterprise Risk Managern im deutschsprachigen Raum

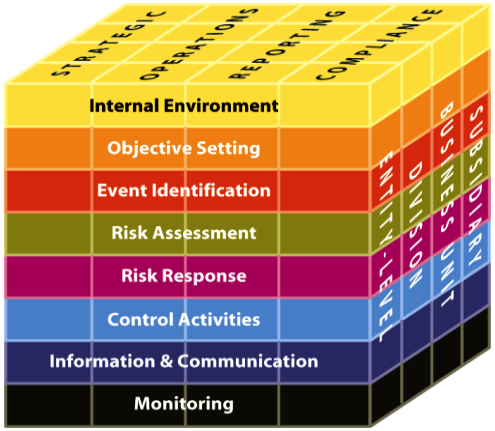
- Größtes unabhängige **Netzwerk von Risikomanagern** außerhalb der Finanzwirtschaft mit mehr als 450 Mitgliedern
- Einzige **Interessenvertretung** für Risikomanager, z.B. in der ISO oder beim IDW
- 15 **Arbeitskreise,** z.B. „IT-Risikomanagement“
- **Regionale** Ansprechpartner
- Zertifizierungsprogramm zum **„Enterprise Risk Manager“**
- **Jahreskonferenz** größter ERM-Kongress in Deutschland
- **Publikationen** in der Fachzeitschrift „ControllerMagazin“ und im Erich-Schmidt-Verlag (Schriftenreihe Risikomanagement)

https://www.rma-ev.org/

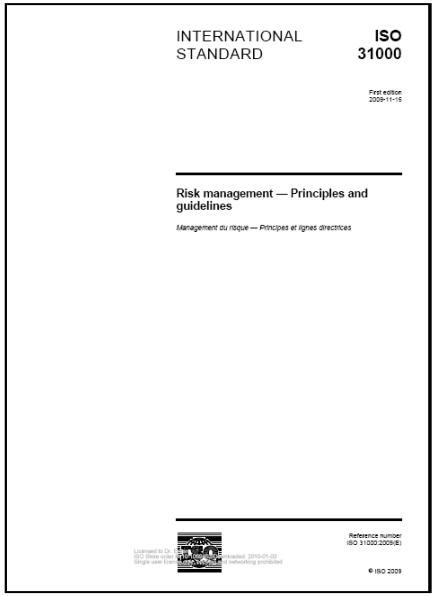
Bedeutung und Entwicklung von COSO ERM, ISO 31000 und anderen relevanten Standards im Risikomanagement

- **Risikomanagement-Standards dienen zur Orientierung und als Rahmen**

USA: COSO
Enterprise Risk Management



Global: ISO 31000
Risk Management


INTERNATIONAL STANDARD
ISO 31000

First edition
2009-11-15

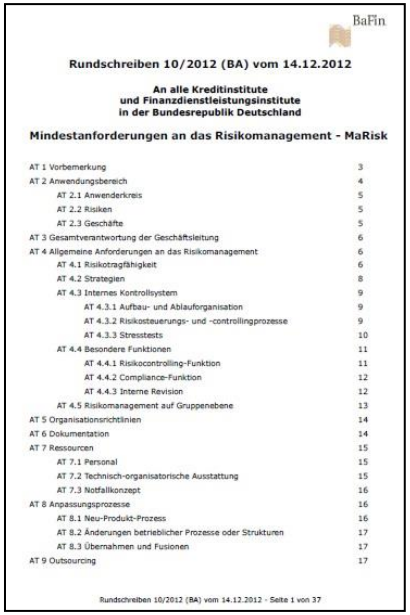
Risk management — Principles and guidelines

Management du risque — Principes et lignes directrices

Reference number
ISO 31000:2009(E)

© ISO 2009

Deutschland: MaRisk
Mindestanforderungen an das Risikomanagement


BaFin

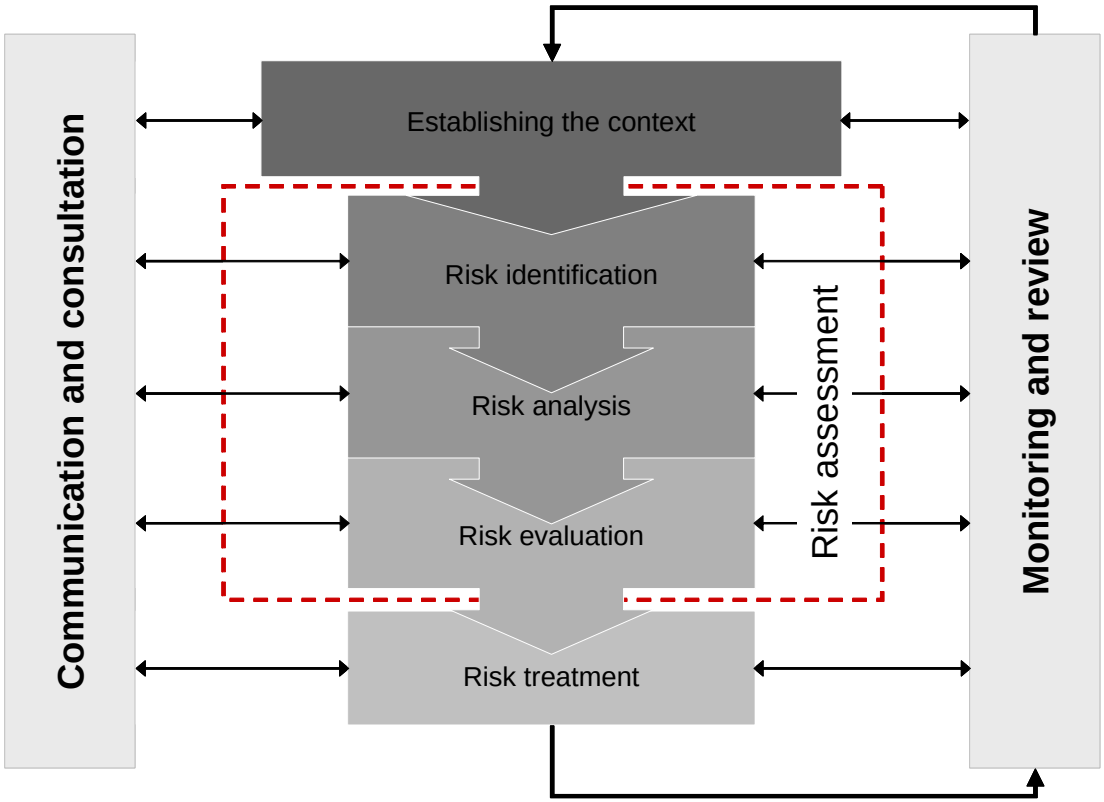
Rundschreiben 10/2012 (BA) vom 14.12.2012

An alle Kreditinstitute
und Finanzdienstleistungsinstitute
in der Bundesrepublik Deutschland

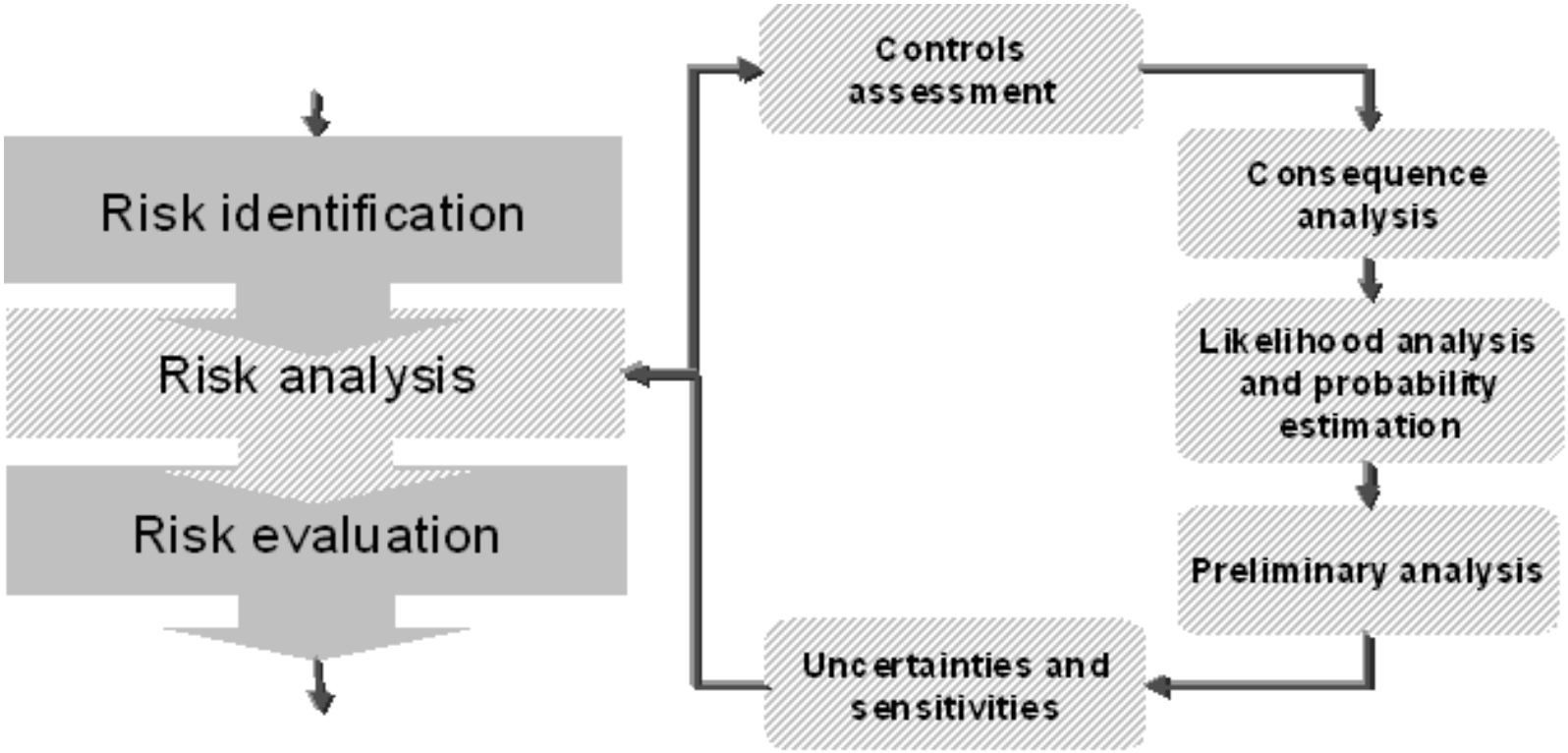
Mindestanforderungen an das Risikomanagement - MaRisk

Rundschreiben 10/2012 (BA) vom 14.12.2012 - Seite 1 von 37

ISO 31000 definiert den gesamten Risikomanagement-Prozess



- **Der Teilprozess „Risk Assessment“ wird in ISO 31010 vertieft**



Zusammenarbeit von RMA und ISACA im Arbeitskreis „IT-Risikomanagement“

- **RMA Arbeitskreis „Risikomanagement“, geschlossene Gruppe**
  - Ziel des Arbeitskreises „Risikomanagement“ ist es, Hilfestellungen für Praktiker im Umfeld des Risikomanagements zu erarbeiten und den Mitgliedern der RMA zur Verfügung zu stellen.

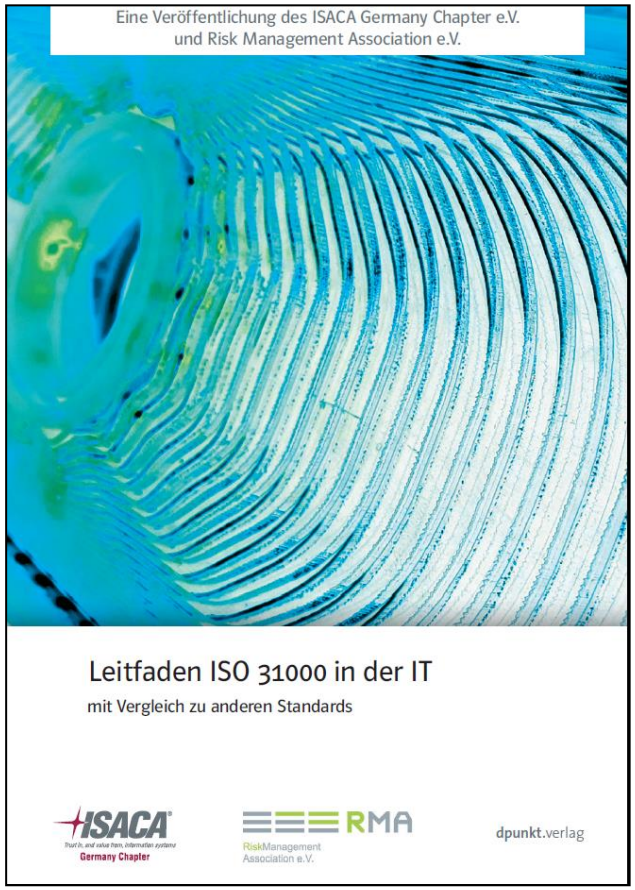
- **ISACA-Fachgruppe „IT-Risikomanagement“**
  - Ziel der Fachgruppe „IT-Risikomanagement“ ist die Erarbeitung von Hilfsmitteln für Praxisfragen bei der Ausgestaltung eines IT-Risikomanagements, die der relevanten Zielgruppe - IT-Verantwortlichen, Risikomanagern, aber auch Linienverantwortlichen - zur Verfügung gestellt werden können.

- **Mitte 2014 Kooperation von RMA mit der ISACA-FG „IT-Risikomanagement“**

Gemeinsamer ISACA-/RMA-Leitfaden zur ISO 31000 in der IT

RMA hat in Kooperation mit dem ISACA Germany Chapter einen „**Leitfaden zur Anwendung der ISO 31000 in der IT mit Vergleich zu anderen Standards**“ veröffentlicht

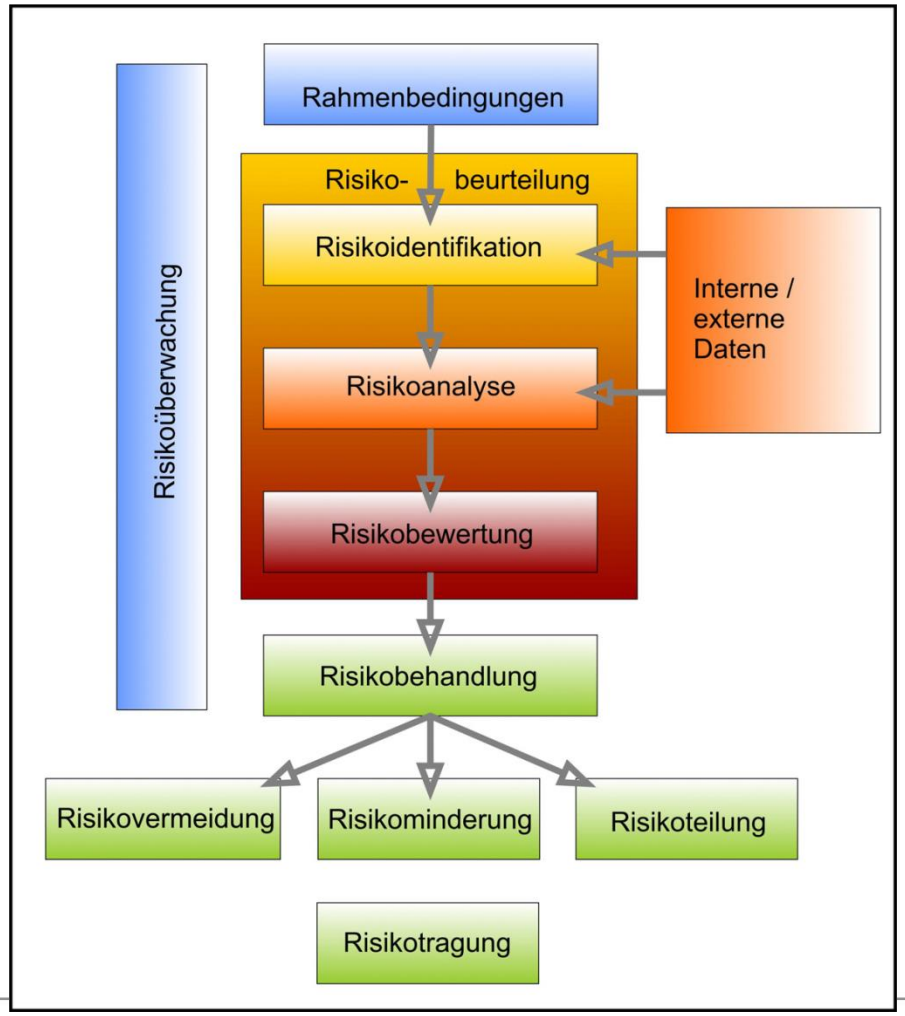
- Dieses Rahmenwerk soll die Komplexität im Standardisierungs- und Methodenumfeld reduzieren
- Schafft mehr Übersicht im Umgang mit dem Thema IT-Risikomanagement



Gemeinsamer ISACA-/RMA-Leitfaden zur ISO 31000 in der IT

- **Zielgruppe**
  - Interne IT-Revisoren
  - IT-Prüfer im Rahmen der Abschlussprüfung
  - IT-Sicherheits-Beauftrage
  - IT-Compliance-Manager
  - IT-Governance-Spezialisten
  - IT-Risikomanager
- **Ziel des Leitfadens**
  - beleuchtet die Vorgaben der ISO 31000 aus einem IT-bezogenen Blickwinkel
  - gibt Hinweise zur praktischen Umsetzung im Bereich der IT
  - die mit praktischen Beispielen unterlegt sind

Gemeinsamer ISACA-/RMA-Leitfaden zur ISO 31000 in der IT



Gemeinsamer ISACA-/RMA-Leitfaden zur ISO 31000 in der IT

- **Risikomanagement-Prozess mit praktischen Beispielen**
  - Risikoidentifikation
    - Als Hilfe zur Identifikation können **interne Quellen** herangezogen werden, dazu zählen:
      - Malware-Statistik des internen Antivirenschutzes
      - Firewall-, Proxy- und IDS-Protokolle über Eindringversuche
      - Incident-Meldungen der Mitarbeiter des Helpdesks
      - Auswertung des Vulnerability- und Patch-Managements
      - Bedrohungen aus Blogs, Foren und sozialen Netzwerken
    - Jedoch sollte man auch die **externe Quellen** intensiv nutzen:
      - Die IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
      - Die Information Security Resources des SANS-Institutes
      - DsiN.de – Deutschland sicher im Netz
      - CERT

Gemeinsamer ISACA-/RMA-Leitfaden zur ISO 31000 in der IT

- **Risikomanagement-Prozess mit praktischen Beispielen**
  - Risikoanalyse
    - Bei der **rein technischen Risikoanalyse** sollten Werkzeuge zum Einsatz kommen, die die vorhandenen Systeme analysieren und eine erste Risikoindikation vornehmen (z.B. in „Ampelfarben“)
      - *nmap/zenmap*
      - *NESSUS*
      - *Microsoft Baseline Security Analyzer*
    - Hierbei sollten interne Analyseergebnisse durch **externe Daten ergänzt** werden, um ein möglichst objektives Bild der Gesamtsituation zu zeichnen
      - Die „Schwachstellenampel“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
      - <kes>/Microsoft-Sicherheitsstudie 2015
      - Informationen der SANS-Organisation

Gemeinsamer ISACA-/RMA-Leitfaden zur ISO 31000 in der IT

- **Risikomanagement-Prozess mit praktischen Beispielen**
  - Risikobewertung
    - Im Bereich der IT-Risiken ist es z.B. sinnvoll, die klassischen Werte der IT-Sicherheit, die auch in der **ISO 27001** zugrunde gelegt werden, als Wertungsmaßstab heranzuziehen: **Vertraulichkeit, Verfügbarkeit, Integrität**.

Grundwert / Bewertungsziffer	Vertraulichkeit	Verfügbarkeit	Integrität
1 unbedeutend			
2 gering			
3 spürbar			
4 kritisch			
5 katastrophal			

Gemeinsamer ISACA-/RMA-Leitfaden zur ISO 31000 in der IT

- **Beurteilung der ISO 31010-Methoden/Techniken (>30) im Kontext der Risikobeurteilung**
  - Risikoidentifikation
  - Risikoanalyse
  - Risikobewertung
  - IT-Eignung
- **Legende**
  - ☑ gut geeignet gemäß ISO 31010
  - ☑☑ sehr gut geeignet gemäß ISO 31010
  - ☒ nicht geeignet gemäß ISO 31010
  - 💻 für die IT geeignet (Wertung der Autoren)
  - 💻💻 für die IT gut geeignet (Wertung der Autoren)

Gemeinsamer ISACA-/RMA-Leitfaden zur ISO 31000 in der IT

Beispiele ISO 31010-Methoden/Techniken

Wahrscheinlichkeits- und Auswirkungsmatrix

- Risikoidentifikation ☑☑
- Risikoanalyse ☑☑
- Risikobewertung ☑
- IT-Eignung 💻💻
- Methodikbeschreibung, etc.

Gemeinsamer ISACA-/RMA-Leitfaden zur ISO 31000 in der IT

Beispiele ISO 31010-Methoden/Techniken

Checklisten

- Risikoidentifikation ☑☑
- Risikoanalyse ☒
- Risikobewertung ☒
- IT-Eignung 💻💻
- Methodikbeschreibung, etc.

Gemeinsamer ISACA-/RMA-Leitfaden zur ISO 31000 in der IT

Beispiele ISO 31010-Methoden/Techniken

Monte-Carlo-Simulation

- Risikoidentifikation ☒
- Risikoanalyse ☒
- Risikobewertung ☑☑
- IT-Eignung 💻
- Methodikbeschreibung etc.

Gemeinsamer ISACA-/RMA-Leitfaden zur ISO 31000 in der IT

- **Implementierung/Anwendung der ISO 31004 unter IT-Gesichtspunkten**
  - Die ISO 31004 ist **kein Standard** im engeren Sinn, sondern **ein** sogenannter **Technical Report**. Als Guidance soll sie den Anwender der ISO 31000 bei der Implementierung unterstützen.
  - Eine wesentliche Rolle spielt dabei die **Integration in die generellen Managementprozesse**, auch in die der IT, ohne dass diese explizit erwähnt wären.
    - Anhang A: Underlying concepts and principles
      - Anwendung in der IT: einheitliche Begriffe und Definitionen finden
    - Anhang B: Application of the principles
    - Anhang C: How to express mandate and commitment
    - Anhang D: Monitoring and review
      - Anwendung in der IT: Überwachung von Systemen, Korrelation von Logging-Daten, Daily Business

Gemeinsamer ISACA-/RMA-Leitfaden zur ISO 31000 in der IT

- **Vergleich mit drei anderen Rahmenwerken/Standards**
  - ISO/IEC 27005:2008
    - ISO 27005 „Information technology - Security techniques - Information security risk management“ aus dem Jahr 2008
    - Sie basiert auf dem **gleichen Vorgehensmodell** (Prozess) und den gleichen Prinzipien wie die ISO 31000 „Risk management - Principles and guidelines“
    - Im Vergleich zur ISO 31000 ist die ISO 27005 eine **Spezialisierung zum Thema operationales Risikomanagement** in Bezug auf das **Management von Informationssicherheitsrisiken**
  - COBIT 4.0 bzw. 4.1
    - COBIT (Control Objectives for Information and related Technology) ist ein Prozessmodell mit 34 Prozessen
    - Ein **Prozess** dieses Frameworks „**Beurteile und manage IT-Risiken**“ beschäftigt sich explizit mit dem Thema Risikomanagement.

Gemeinsamer ISACA-/RMA-Leitfaden zur ISO 31000 in der IT

- **Vergleich mit drei anderen Rahmenwerken/Standards**
  - BSI IT-Grundschutz-Standard 100-3
    - Der Standard 100-3 des BSI fokussiert auf die Risikoanalyse als Teil des Risikomanagementprozesses.
    - Er beinhaltet die **konkrete Beschreibung einer Methodik**, wie **aufbauend** auf den Grundschutz-Katalogen und den BSI-Standards 100-1 und 100-2, eine **vereinfachte Risikoanalyse für Risiken der Informationsverarbeitung** durchgeführt werden kann.
    - Die **Methodik beinhaltet** dabei lediglich eine **implizite Bewertung der Wahrscheinlichkeit und Auswirkungen** von Risiken im Rahmen der Ermittlung und Bewertung von Gefährdungen
    - Ist eine **explizite Bewertung** der **Eintrittswahrscheinlichkeit und Auswirkungen eines Risikos** gefordert, ist der Einsatz des BSI-Standards 100-3 jedoch ohne weitere Modifikationen der **Methodik nicht zu empfehlen**

Gemeinsamer ISACA-/RMA-Leitfaden zur ISO 31000 in der IT

- Interessenten können den neuen Leitfaden zu „ISO 31000 in der IT“ kostenlos bestellen bzw. herunterladen
  - RMA www.rma-ev.org/Veroeffentlichung-zumDownload.696.0.html oder
  - ISACA https://isaca.de/sites/pf7360fd2c1.dev.team-wd.de/files/attachements/2014_11_isaca-leitfadenanwendungderiso31000inderit.pdf