Zürcher Hochschule
für Angewandte Wissenschaften

School of
Management and Law

AACSB ACCREDITED
Since 2015

Herzlich Willkommen

zum 106. ABL-Forschungslunch

Risikobasierte Entscheide im Recht - Fokus Datenschutz

Volker Dohr

Building Competence. Crossing Borders.

Prof. Dr. iur. Philipp Egli, Forschungsverantwortlicher ABL

Vorstellung

Volker Dohr, Rechtsanwalt (DE), CIA, Dozent

Berufserfahrung

- 2022 - heute: Founding Partner impunix
- 2021 - 2022: Founding Partner IXAR Legal AG
- 2019 - 2021: Partner einer Wirtschaftskanzlei
- 2016 - heute: Dozent ZHAW
- 2013 - 2018: AMAG Group AG (Legal & Compliance)
- 2013 - 2013: SoftwareOne AG (SAM-Consulting)
- 2007 - 2013: Swisscom AG (IT-Governance, Risk, Audit)
- 2002 - 2007: Software Quality Systems Schweiz (IT-Compliance-Consultant)
- 2001 - 2002: Computer Science Corporation (IT-Consultant)

Schwerpunkte:

- Compliance- und Corporate Governance
- Wettbewerbs- und Kartellrecht
- KFZ- und Vertriebsrecht
- IT, Datenschutz und Datensicherheit
- Marketing- und IP-Recht
- Dozent für IT-Recht, Datenschutz, Compliance / Studiengangleiter CAS Compliance Investigation

Risikobasierte Entscheide im Recht Fokus Datenschutz

- Mit seiner Zwischenverfügung vom 27. Oktober 2022 hat das Bundesverwaltungsgericht den risikobasierten Ansatz im Datenschutz bestätigt und die Nutzung von ausländischen Cloud Diensten in der Bundesverwaltung explizit (jedoch nur vorläufig) erlaubt, sofern vor dem Einsatz umfassende risikobasierte Abklärungen getroffen und dokumentiert worden sind.
- Wie dieses Beispiel zeigt, fördert der Datenschutz die Bedeutung und das Verständnis von Risikomanagement im Recht. Darüber hinaus sind risikobasierte Entscheidungen ein Trend, der sich seit längerem abzeichnet und sich im Recht an verschiedenen Orten zunehmend durchsetzt. So hat das Bundesgericht bereits vor gut 10 Jahren in der Business Judgement Rule Entscheidung von 2012 (4A_74/2012) den Weg zu risikobasiertem Handeln vorgezeichnet. Welche Methodik praktikabel ist, wie die Vorgaben rechtssicher eingesetzt werden und in der Praxis umgesetzt werden können, zeigt das Referat von Volker Dohr auf, beginnend mit der Entwicklung von risikobasierten Entscheidungen und Vertragsklauseln in der Vergangenheit und heute. Der Ausblick befasst sich mit dem neuen Schweizer Datenschutzgesetz, das im September 2023 in Kraft treten wird.

- Volker Dohr ist Dozent an der Abteilung Business Law. Er ist als Jurist und Rechtsanwalt tätig und hat viele Jahre Berufserfahrung in der Finanz-Informatik.

Agenda

- Cases-Behörden-Gerichtsentscheide
- Gesetzliche Regulierung zum Risiko
- Risikobegriff – in Ökonomie und Recht
- Risikomanagement und Audit Risiko
- Fazit

Unternehmen die Risiken bewusst oder unbewusst eingegangen sind.

Risiko: Betrug

BARINGS

- 1995 : Devisenhändler **Nick Leeson** hatte mit betrügerischen Spekulationen der Bank Barings einen **Handelsverlust** von **1.4 Mrd. US-Dollar** beschert.
- Das Traditionshaus ging daraufhin **nach 233 Jahren** unter und für ein Pfund an die ING.
- Nick Leeson gilt inzwischen als eine kleine Nummer.

SOCIETE GENERALE

- 2008: Jérôme Kerviel, ein **Händler** der Bank Société Général, dem vorgeworfen wird, einen **Verlust von 4.9 Mrd. €** verursacht zu haben.
- In einem Interview sagt er: „*Die Chefetage interessierte sich nicht für meine Methoden, aber mit dem Ergebnis ist sie zufrieden.“*
- Zitat von D. Ostergard zum Managementverhalten: „*The outcome is business decisions and practices which lack integrity, designed to meet short-term earning targets at any cost.” ..*
- *..Once the losses started mounting, the bank blamed the works of a bad apple, sacked him and promised to spend* ***€ 100M. to improve controls.***

UBS

- 2011: Kweku **Adoboli**: Investment Manager and former stock trader.
- “illegally trading” with **US$2 billion** (GB£1.3 billion) loss as a trader for Swiss investment bank UBS.

Risiko: Beihilfe zu Steuerdelikten

UBS: Umwälzungen am Hotspot Miami

11.08.2020

Die Büros der **UBS** im Finanzdistrikt von Miami, leeren sich: Seit die Schweizer Grossbank in diesem Jahr begonnen hat, ihre Listen mit lateinamerikanischen Wealth-Management-Kunden nach **Compliance**-Risiken zu durchforsten, hat unter den Kundenberatern ein eigentlicher Exodus begonnen.

Risiken: Korruption, Geldwäscherei, Sanktionen

https://www.finews.ch/news/banken/42442-ubs-miami-venezuela-compliance-fim-vermoegensverwalter

Risiko: Datenschutz

Hohe Bussgelder in USA und Europa:

140.- Mio. $ (25.5.22)

amazon

750 Mio. € (30.7.21)

405 Mio. € (5.9.22)

90 Mio. € (6.1.22)

Risiko: Softwarefehler - Datenleck bei CSS

- CSS: Mehrere Rechnungen mit Gesundheitsdaten werden im Jahr 2019 publik, da diese mit den falschen Kundenkonten in der App verknüpft wurden.
- Es wird von über 1000 Rechnungen ausgegangen
- CSS versendet pro Jahr 17 Mio. Rechnungen)

- DS-Gesetz: **Verpflichtung zu „angemessenem“** und am **„Stand der Technik“** orientierten Datenschutz.

- Medienmitteilung: Es waren nur 0.7 Promille der Rechnungen betroffen.
- Frage: Sind 0.7 Promille Fehler angemessen? Oder wurde das Risiko falsch eingeschätzt?

Quelle: blick.ch und SRF.ch, 27. August 2019

Business Judgment Rule

Gemäss der in den USA entwickelten, und in Europa und der Schweiz anerkannten, Business Judgment Rule, handelt ein Geschäftsführer **sorgfältig:**

1. wenn er bei einer Entscheidung in KEINEM Interessenkonflikt stand,
2. angemessen und ausreichend informiert war oder
3. die Überzeugung besteht, im besten Interesse der Gesellschaft zu handeln.

Kernaussage der Business Judgment Rule ist, dass Fehlentscheide, die zu Verlusten der Gesellschaft führen, zur Geschäftsführung gehören und nicht per se pflichtwidrig sind. Am Markt teilzunehmen heisst gerade Risiken eingehen und daher werden auch sorgfältig getroffene Entscheide sich später als Fehler herausstellen.
Die Richter sollen deshalb nicht retrospektiv über die wirtschaftliche Richtigkeit von Geschäftsleitungsentscheiden urteilen, sondern der Geschäftsführung einen Ermessensspielraum zubilligen.

Urteil des Bundesgerichts vom 28. August 2013. Wegen Beschwerde des Management gegen das vorinstanzliche Urteil iS. Darlehensgewährung.

Keinen Berufung auf die Business Judgement Rule:

….Mit anderen Worten lag in der Unterlassung der sich aufdrängenden Abklärungen eine **offensichtliche Unsorgfalt.** Die Entscheide wurden auf offensichtlich ungenügender Informationsbasis getroffen. Damit durfte die Vorinstanz eine Pflichtverletzung bejahen, ohne dass sie weiter der Frage nachgehen musste, ob die **Darlehensgewährung** unter anderen Gesichtspunkten bzw. bei einer Abwägung von Chancen und Risiken aus damaliger Sicht dennoch als richtig erscheint (vgl. in diesem Sinn: Vogt/Bänziger, Das Bundesgericht anerkennt die Business Judgement Rule als Grundsatz des schweizerischen Aktienrechts, GesKR 4/2012 S. 607 ff., 617).

Schwyz, Kantonsgericht
Urteil vom 18. Mai 2020

….Nach konstanter Rechtsprechung des Bundesgerichts **haben sich die Gerichte Zurückhaltung aufzuerlegen bei der nachträglichen Beurteilung von Geschäftsentscheiden**, die in einem **einwandfreien, auf einer angemessenen Informationsbasis beruhenden und von Interessenskonflikten freien Entscheidprozess zustande gekommen sind.** Sind diese Voraussetzungen erfüllt, prüft das Gericht den Geschäftsentscheid in inhaltlicher Hinsicht lediglich darauf, ob er als vertretbar erscheint.

Andernfalls rechtfertigt es sich aber nicht, bei der Prüfung der Sorgfaltspflichtverletzung besondere Zurückhaltung zu üben und nur zu prüfen, ob der Entscheid noch im Rahmen des Vertretbaren liegt.

Vielmehr reicht es dann aus, dass ein Geschäftsentscheid in der gegebenen Situation bei freier bzw. umfassender Prüfung als fehlerbehaftet erscheint (BGer, Urteil 4A_259/2016, 4A_267/2016 vom 13. Dezember 2016 E. 5.1 mit weiteren Hinweisen auf die bundesgerichtliche Rechtsprechung; sog. „Business Judgement Rule“).

BVerwG - Zwischenverfügung vom 27. Oktober 2022 “A gegen Bundeskanzlei wegen Datenschutz, MS365 u.a.”

Bundesverwaltungsgericht
Tribunal administratif fédéral
Tribunale amministrativo federale
Tribunal administrativ federal

Abteilung I

Postfach
CH-9023 St. Gallen
Telefon +41 (0)58 465 25 02
Fax +41 (0)58 465 29 80
www.bundesverwaltungsgericht.ch

Geschäfts-Nr. A-661/2022
min/kob

Zwischenverfügung vom 27. Oktober 2022

In der Beschwerdesache

Parteien
A._____,
Beschwerdeführer,

gegen

Schweizerische Bundeskanzlei BK,
Bundeshaus West, 3003 Bern,
Vorinstanz,

Gegenstand
Öffentlichkeitsprinzip und Datenschutz;
Rechtsverweigerung,

Das BVerwG hält die getroffenen Massnahmen des Bundes für ausreichend, wonach: Die Schweizerische Bundeskanzlei …mit Schreiben vom 21. Januar 2022 mitteilt, dass die Auslagerung von Daten und von deren Bearbeitung rechtskonform erfolgen muss, was in jedem Fall durch eine **vorgängige Prüfung der Rechtskonformität, einer Risikoanalyse und – bei Personendaten – einer Datenschutzfolgeabschätzung sichergestellt werde.**

(S. 12) … im Übrigen ist noch nicht ersichtlich, dass es im Rahmen des Projekts zur Einführung bestimmter Microsoft 365-Applikationen in der Cloud, das sich derzeit noch in der Konzeptphase befindet, auch ältere Daten neu elektronisch abgelegt und/oder in einer Cloud gespeichert werden sollen.
Nach dem Gesagten droht derzeit keine (weitere) Auslagerung von Personendaten durch die Vorinstanz in eine (ausländische) Public Cloud und somit auch keine (weitere nicht wieder gut zu machende) Offenbarung gegenüber Dritten.

«Fazit: es bleibt kein Raum für vorsorgliche Massnahmen, da kein Risiko besteht»

Geldbussen für DSGVO-Verstösse wegen ungenügender Risikobeurteilung

DSFA= Datenschutz Folge Abschätzung)

Datum	Bussgeld	Unternehmen	Land	Zusammenfassung
17.11.2022	**800.000 €**	Discord Inc.	FR	Zu lange Aufbewahrung von Daten, keine DSFA, unsichere Passwörter, keine datenschutzfreundliche Voreinstellungen.
28.09.2021	**496.746 €**	Ferde AS	NO	Keine Rechtsgrundlage für Übermittlung nach China, fehlende Risikoanalyse und mangelnde Schutzmassnahmen.
27.07.2021	**2.520.000 €**	MERCADONA, S.A.	ES	Gesichtserkennungssystem in 40 Supermärkten erfasste uneingeschränkt jede Person. Keine DSFA.
22.06.2021	**84.000 €**	Gemeinde Bozen	IT	Umfassende Erfassung der Internetnutzung von Beschäftigten, Verletzung der Informationspflicht, keine DSFA.
17.12.2020	**240.832 €**	ID Finance Poland Sp. z o.o.	PL	Inadäquate Schutzmassnahmen und verzögerte Benachrichtigung nach Datenpanne mit hohem Risiko.
03.12.2020	**1.447.527 €**	Aleris Sjukvård AB	SE	Fehlende Bedarfs- und Risikoanalyse für den Zugriff auf Patientendaten und zu weitreichende Berechtigungen.

Agenda

- Cases-Behörden-Gerichtsentscheide
- Vorgaben und Regulierung zum Risiko
- Risikobegriff – in Ökonomie und Recht
- Risikomanagement und Audit Risiko
- Fazit

Begriffe
Governance, Risk & Compliance

Governance → **Umfassende Steuerung der Organisation**

Risk Management → $Planungssicherheit = f(Ziele, Unsicherheit)$

Compliance Management → **System zur Einhaltung** relevanter Vorgaben

Begriffe – Risk Management

Risk
Management

System zur Erkennung und dem Umgang mit der Unsicherheit, um Planungssicherheit zu erzielen.

$$Planungssicherheit = f\,(Ziele, Unsicherheit)$$

Es umfasst die **permanente**, **systematische** Risikoidentifikation, **-beurteilung** und **-kontrolle** in einem **ganzheitlichen** Sinn und dient damit der Erkennung von Chancen und Gefahren des im Einzelnen eingegangen Risikos für das Unternehmen.

Mit der „**Compliance**“ bestehen dabei Überschneidungen in Bezug auf Rechts- und Reputationsrisiken.

Explizit für Banken geregelt in: Art. 12 Abs. 2 BankV.

Rechtliche Pflichtenkategorien – Governance, Risk & Compliance Management (GRC)

OR 716a Abs. 1

Der VR hat …

1. Oberleitung der Gesellschaft und die Erteilung …Weisungen;
2. Festlegung der Organisation (Anm: Aufbau- und Ablauforganisation);
3. **Ausgestaltung des Rechnungswesens, der Finanzkontrolle sowie der Finanzplanung,** … wenn dies notwendig ist.
5. **Oberaufsicht** über die mit der Geschäftsführung betrauten Personen, namentlich im Hinblick auf die **Befolgung der Gesetze**, Statuten, Reglemente und Weisungen;

Rechtliche Pflichten
Governance, Risk & Compliance Management (GRC)

OR 717 Abs. 1

VR und Management haben:

1. **Sorgfaltspflicht**
2. **Treuepflicht**

Ziel:
Verhaltenssteuerung und Verantwortlichkeit klarstellen
(Organhaftung: Art. 754 I & II OR)

Regelungs-Kanon:

- Regelung & Steuerung durch Prinzipiennormen
- Konkretisierung im Einzelfall
- Sanktionierung durch Gerichte

Rechtliche Pflichtenkategorien – Die Sorgfaltspflicht von VR und Management Governance, Risk & Compliance Management (GRC)

OR 717 Abs. 1

Sorgfaltspflicht

- Handeln **"mit aller Sorgfalt"** im **"Interessen der Gesellschaft"** (Art. 717 Abs. 1 OR)

- objektivierter, individualisierter Sorgfaltsmassstab
- Sorgfalt und Kenntnisse/Fähigkeiten – Beizug von Spezialisten
- Sorgfalt bei der Annahme des Mandats als VR/Manager
- Sorgfalt bei Geschäftsentscheiden und im Umgang mit Risiken
  - (vgl. BGer 4A_74/2012, E. 5; BGer 4A_306/2009, E. ***business judgment rule*** 7.2.4; BGer 4C.201/2001, E. 2.1.2)
- Sorgfalt bei der Verwendung von Gesellschaftsvermögen
  - Gewährung von Darlehen (BGer 6B_54/2008)
  - Bezahlung von Abgangsentschädigungen (BGer 4A_174/2007 und BGer 4A_188/2007)
  - Festlegung der Vergütungen (vgl. Art. 717 Abs. 1bis VE-OR 2014)
- Sorgfalt betreffend Erhebung einer Verantwortlichkeitsklage (siehe Art. 756 Abs. 1 OR) und allgemein bei der Geltendmachung von Ansprüchen
- Sorgfalt bei der Organisation und Kontrolle

Rechtliche Pflichtenkategorien – Die Revisionsstelle
Governance, Risk & Compliance Management (GRC)

OR 728a Abs. 1

Revisionsstelle

Revisionsstelle , Gegenstand und Umfang der Prüfung

Abs. 1:

- ***Die Revisionsstelle prüft, ob:***
  - *Nr. 1 die Jahresrechnung und gegebenenfalls die Konzernrechnung den gesetzlichen Vorschriften, den Statuten und dem gewählten Regelwerk entsprechen;*
  - *Nr. 2.der Antrag des Verwaltungsrats an die Generalversammlung über die Verwendung des Bilanzgewinnes den gesetzlichen Vorschriften und den Statuten entspricht;*
  - ***Nr. 3. ein internes Kontrollsystem (IKS) existiert.***

Abs. 2:

- ***Die Revisionsstelle berücksichtigt bei der Durchführung und bei der Festlegung des Umfangs der Prüfung - das interne Kontrollsystem.***

Rechtliche Pflichtenkategorien – Sektorregulierung
Governance, Risk & Compliance Management (GRC)

Versicherungsaufsichtsgestz (VAG) - Art. 22

2. Abschnitt Risikomanagement:

1. Das Versicherungsunternehmen muss so organisiert sein, dass es insbesondere alle wesentlichen Risiken erfassen, begrenzen und überwachen kann.

2. Der Bundesrat erlässt **Vorschriften** über Ziel, Inhalt und Dokumentation des **Risikomanagements**.

3. Die FINMA regelt die **Überwachung** d**er Risiken durch das Versicherungsunternehmen**.

Risikomanagement BankV
Art. 12 II BankV

BankV - Art. 12 II

Risikomanagement

Das Risikomanagement bezweckt die **umfassende** und **systematische Steuerung** und **Lenkung** von Risiken.

Internes Kontrollsystem

Es umfasst die **permanente**, **systematische Risikoidentifikation**, **-beurteilung** und **-kontrolle** (und) in einem **ganzheitlichen** Sinn dient es damit der (nachhaltigen) **Erkennung** von **Chancen** und **Gefahren** des im Einzelnen eingegangen Risikos für das Unternehmen.

Art. 12 Abs. 2 BankV

Risikomanagement im revDSG ab 1.9.2023
Datenschutz-Gesetz (DSG) und Datenschutz-Verordnung (DSV)

DSG

Art. 8 – Datensicherheit

1) Der Verantwortliche und der Auftragsbearbeiter gewährleisten **durch geeignete** technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit.

DSV

Art. 1 - Grundsätze

1 Zur Gewährleistung einer **angemessenen** Datensicherheit müssen der Verantwortliche und der Auftragsbearbeiter den **Schutzbedarf** der Personendaten bestimmen und die im Hinblick auf das Risiko geeigneten technischen und organisatorischen Massnahmen festlegen.

2 Der **Schutzbedarf der Personendaten** wird nach den folgenden **Kriterien** beurteilt: a.) Art der bearbeiteten Daten; b.) Zweck, Art, Umfang und Umstände der Bearbeitung.

3 Das **Risiko für die Persönlichkeit** oder die Grundrechte der betroffenen Person wird nach den folgenden **Kriterien** beurteilt:

a.) **Ursachen** des Risikos; b.) hauptsächliche **Gefahren**; c.) ergriffene oder vorgesehene **Massnahmen**, um das Risiko zu verringern; d.) **Wahrscheinlichkeit** und **Schwere** einer Verletzung der Datensicherheit trotz der ergriffenen oder vorgesehenen Massnahmen.

4 Bei der **Festlegung der technischen und organisatorischen Massnahmen** werden zudem die folgenden **Kriterien** berücksichtigt: a.) Stand der Technik; b.) Implementierungskosten.

Risiko-Kontroll-Matrix

Das zentrale Instrument zur Enthaftund der Entscheider

Prozess	Finanzen						
Prozessziel	Die Konten im Bereich Finanzen werden im Rechnungswesen korrekt und vollständig geführt.						
Primäre Aktivitäten: Einkauf, Lager, Verkauf Sekundäre Aktivitäten: Personalmanagement/Human Resources (HR); Informationstechnologie (IT); Finanzen			Prozessverantwortlicher: Stellvertreter: Datum: Beispiele von Konten, die betroffen sein könnten: Kasse, Bank, Eigenkapital etc.				
	Risikoanalyse		Steuerungs- und Kontrollmassnahmen				
Teilprozesse/ Teilprozessziele		Risikofaktoren/ Risikobeschreibung	Rating	Massnahmen/ Kommentare	Verantwortliche(r)	Typ (manuell/ automatisch; präventiv/ detektiv)	Beurteilung/ Schlussfolgerung (ok/nein, Kommentar)
Darstellung im Jahresabschluss: Kassenbestand							
Der Kassenbestand ist korrekt und vollständig.	1	Der Kassenbestand ist fehlerhaft oder nicht vorhanden.	mittel	• Die Kasse ist physisch gesichert (klare Regelung des Zugriffs bzw. Zugangs). • Der Kassenbestand wird regelmässig physisch durch eine neutrale Person überprüft (periodischer Kassensturz) und mit der Buchhaltung abgestimmt. • Der Kassenbestand wird zum Schutz vor grösserem Verlust grundsätzlich möglichst niedrig gehalten.	Kassier, Buchhaltung	m, p/d	Nein: Der Mitarbeiter, welcher die Kasse führt, nimmt gleichzeitig deren buchmässige Fortschreibung vor.
	2	Die Bargeldbezüge werden nicht oder falsch verbucht.	mittel	Die Kasseneinnahmen und -bezüge werden laufend im Kassenprotokoll registriert oder eingetragen und mit dem Rechnungswesen abgestimmt.	Kassier	m, p/d	ok
	3	Grosse Bargeldmengen werden ohne Genehmigung bezogen.	gering	• Die Verbuchung der Kassenbewegungen erfolgt nur mit Genehmigung der transaktionsverantwortlichen Person. • Die Bargeldbezüge sind durch eine Kompetenz- und Unterschriftenregelung im Unternehmen betraglich limitiert. • Transaktionen des Unternehmens werden zudem möglichst bargeldlos abgewickelt.	Kassier	m, p	ok
	4	Die Bareinnahmen werden nicht oder falsch verbucht.	mittel	• Der Kassenbestand wird regelmässig physisch überprüft (periodischer Kassensturz) und mit der Buchhaltung abgestimmt. • Die Kasseneinnahmen und -bezüge werden sofort im Kassenprotokoll registriert oder eingetragen.	Kassier	m, p/d	ok
	5	Transaktionen in Fremdwährung werden zur falschen Kurswährung abgewickelt.	gering	Fremdwährungskurse werden gemäss Unternehmensrichtlinien verbucht.	Kassier	m, p	ok
	6	Es liegt keine Funktionstrennung zwischen Kassenführung und Verbuchung vor.	gering	Eine entsprechende Funktionstrennung wird eingerichtet.	Kfm. Leiter	m, p	ok
Darstellung im Jahresabschluss: Bankkonti							
Die Bankkonti sind korrekt und vollständig erfasst.	7	Die Bankkonti sind fehlerhaft oder nicht vorhanden; die Transaktionen werden falsch verbucht.	mittel	Die Bank- und Postkontoauszüge werden periodisch mit der Finanzbuchhaltung abgestimmt. Etwaige Differenzen werden zeitnah geklärt und korrigiert.	Buchhalter	m, d	ok
	8	Nicht genehmigte Transaktionen werden durchgeführt.	mittel	• Die Transaktionen bedürfen einer schriftlichen Genehmigung (anhand Unterschriftsregelung). • Zudem besteht eine klare Regelung der Verantwortlichkeiten und Kompetenzen im Hinblick auf die Geldkonten des Unternehmens. • Mutationsrechte im Bankenstamm sind auf zwei Personen eingeschränkt. • Unterschriftenregelungen werden periodisch vom Leiter Finanzen überprüft.	Linienvorgesetzter, Leiter Finanzen	m/a, p/d	ok
	9	Die Fremdwährungsbewertungen sind fehlerhaft.	mittel	Die Fremdwährungskonten werden periodisch überprüft und bei Bedarf neu bewertet.	Leiter Finanzen	m, d	ok
	10	Zahlungen werden falsch ausgelöst.	mittel	• Die Zahlungen müssen von zwei Personen ausgelöst werden. Als Beleg dient das Zahlungsjournal. • Die Möglichkeit der Zahlungsauslösung wird auf wenige Personen beschränkt.	Controller, Buchhaltung	m/a, p	Vier-Augen-Prinzip bei Zahlungsauslösung fehlt.
	11	Es liegt keine Funktionstrennung zwischen Stammdatenbearbeitung (Bankenstamm) und Zahlungen vor.	gering	Eine entsprechende Funktionstrennung wird eingerichtet.	Kfm. Leiter	m, p	ok

Hiermit bestätige ich, dass…

- ✓ alle Angaben korrekt und vollständig sind.
- ✓ die Prozessziele erreicht wurden.
- ✓ keine wesentlichen Falschdarstellungen

Datum: Unterschrift:

Bestätigungsvermerk der letzten Revision

Ziele

Risiken

Risikowertung

Kontrollen (Massnahmen) zur Risikobegrenzung

Verantwortlicher

Kontrolltyp

Review der Wirksamkeit

Agenda

- Cases-Behörden-Gerichtsentscheide
- Vorgaben und Regulierung zum Risiko
- Risikobegriff – in Ökonomie und Recht
- Risikomanagement und Audit Risiko
- Fazit

Risikomanagement – Risiko

Risiko *beschreibt die Unsicherheit in Bezug auf in der Zukunft liegende* ungewisses *Ereignisse.*

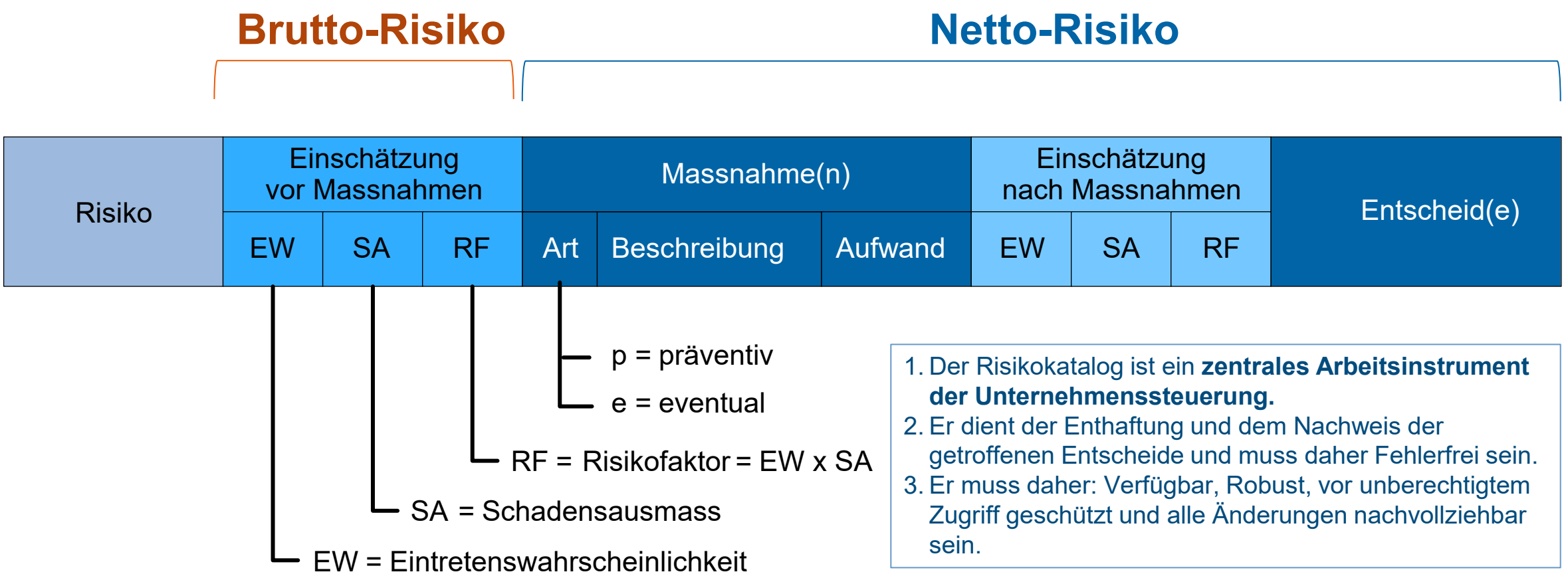
$$Planungssicherheit = f\,(Ziele, Unsicherheit)$$

Mit Risikomanagement soll die Zukunft ins jetzt verlegt werden.

Agenda

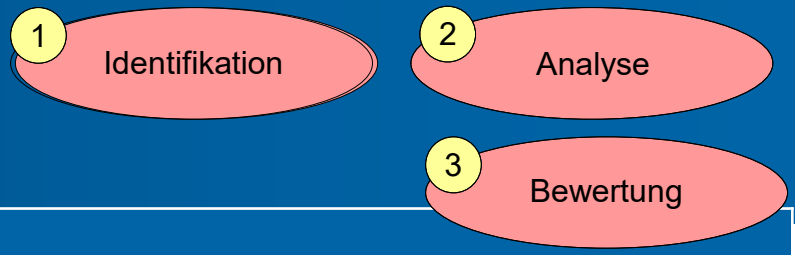
- Cases-Behörden-Gerichtsentscheide
- Vorgaben und Regulierung zum Risiko
- Risikobegriff – in Ökonomie und Recht
- Risikomanagement und Audit Risiko
- Fazit

Risikomanagement
Brutto und Netto - Risiko



1. Der Risikokatalog ist ein **zentrales Arbeitsinstrument der Unternehmenssteuerung.**
2. Er dient der Enthaftung und dem Nachweis der getroffenen Entscheide und muss daher Fehlerfrei sein.
3. Er muss daher: Verfügbar, Robust, vor unberechtigtem Zugriff geschützt und alle Änderungen nachvollziehbar sein.

Risikomanagement
Praxis der Risikoidentifikation



Vorgehen	Methode
Risiko-Workshop	**Kreativitätstechniken**: Brainstorming, Delphi-Technik, Morphologische Matrix **Szenario-Analysen:** Root Cause, Fehlerbaum und Ablaufanalyse, Worst-Case-Szenario **Annahmenanalyse:** Annahmen und Hypothesen hinterfragen
Studium ähnlicher Projekte	z.B. Betriebsanlagen vor Ort besichtigen
Besichtigung- und Organisationsanalyse	Projektumfeld und Unternehmensorganisation hinterfragen
Dokumentationsanalyse	alle für das Projekt relevanten Dokumente reviewen
Risiko-Checkliste(n)	Literatur, Berater, Experten
Indikatoren-Analyse	Critical Incidents-Reporting Systems, Change Based Risk Management
Gefährdungsanalyse	FMEA, Gefährdungsanalysen, HAZOP, HACCP
Statistische Analyse	Standardabweichung, Vertrauensintervall, Monte-Carlo-Simulation

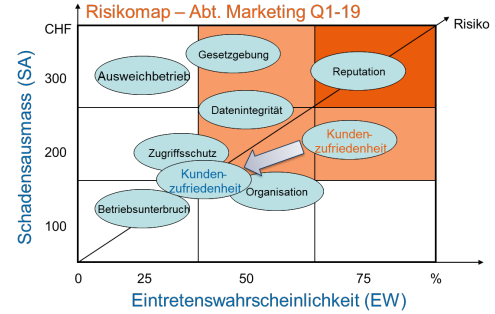
Dokumentation:
- Ergebnisse werden im **Risikokatalog** festgehalten.
- zur **Enthaftung** sollte zudem ein Protokoll erstellt werden.

Risikomanagement
Wie entsteht die Risikomatrix

Eintrittswahrscheinlichkeit (EW) X Schadensausmass (SA) = Risiko (Matrix)

Eintrittswahrscheinlichkeiten			
Farbe	Verbale Umschreibung	Frequenz	Rel. Häufigkeit [%]
Rot	Häufig	1 mal in 0 bis 3 Jahren	33 bis 100
	Gelegentlich	1 mal in 3 bis 6 Jahren	17 bis 33
Gelb	Selten	1 mal in 5 bis 10 Jahren	10 bis 20
	Unwahrscheinlich	1 mal In 10 bis 30 Jahren	3 bis 10
Grün	Praktisch unmöglich	1 mal in 30 oder mehr Jahren	Kleiner 3

Relevanzklasse[79]	Wirkung auf Risikotragfähigkeit	Erläuterungen
1	Unbedeutendes Risiko	Unbedeutende Risiken, die weder Jahresüberschuss noch Unternehmenswert spürbar beeinflussen
2	Mittleres Risiko	Mittlere Risiken, die eine spürbare Beeinträchtigung des Jahresüberschusses bewirken
3	Bedeutendes Risiko	Bedeutende Risiken, die den Jahresüberschuss stark beeinflussen oder zu einer spürbaren Reduzierung des Unternehmenswertes führen
4	Schwerwiegendes Risiko	Schwerwiegende Risiken, die zu einem Jahresfehlbetrag führen und den Unternehmenswert erheblich reduzieren
5	Bestandsgefährdendes Risiko	Bestandsgefährdende Risiken, die mit einer wesentlichen Wahrscheinlichkeit den Fortbestand des Unternehmens gefährden



School of Management and Law

Risikomanagement
Die Eintrittswahrscheinlichkeit

Eintrittswahrscheinlichkeit (EW)

Eintrittswahrscheinlichkeiten			
Farbe	Verbale Umschreibung	Frequenz	Rel. Häufigkeit [%]
Rot	Häufig	1 mal in 0 bis 3 Jahren	33 bis 100
	Gelegentlich	1 mal in 3 bis 6 Jahren	17 bis 33
Gelb	Selten	1 mal in 5 bis 10 Jahren	10 bis 20
	Unwahrscheinlich	1 mal In 10 bis 30 Jahren	3 bis 10
Grün	Praktisch unmöglich	1 mal in 30 oder mehr Jahren	Kleiner 3

Relevanzeinschätzungen

- Scoring-Modelle
- ABC/XYZ-Analysen
- Ratings

Risikomanagement:
Das Schadensausmass

Schadensausmass (SA)

Relevanzklasse[79]	Wirkung auf Risikotragfähigkeit	Erläuterungen
1	Unbedeutendes Risiko	Unbedeutende Risiken, die weder Jahresüberschuss noch Unternehmenswert spürbar beeinflussen
2	Mittleres Risiko	Mittlere Risiken, die eine spürbare Beeinträchtigung des Jahresüberschusses bewirken
3	Bedeutendes Risiko	Bedeutende Risiken, die den Jahresüberschuss stark beeinflussen oder zu einer spürbaren Reduzierung des Unternehmenswertes führen
4	Schwerwiegendes Risiko	Schwerwiegende Risiken, die zu einem Jahresfehlbetrag führen und den Unternehmenswert erheblich reduzieren
5	Bestandsgefährdendes Risiko	Bestandsgefährdende Risiken, die mit einer wesentlichen Wahrscheinlichkeit den Fortbestand des Unternehmens gefährden

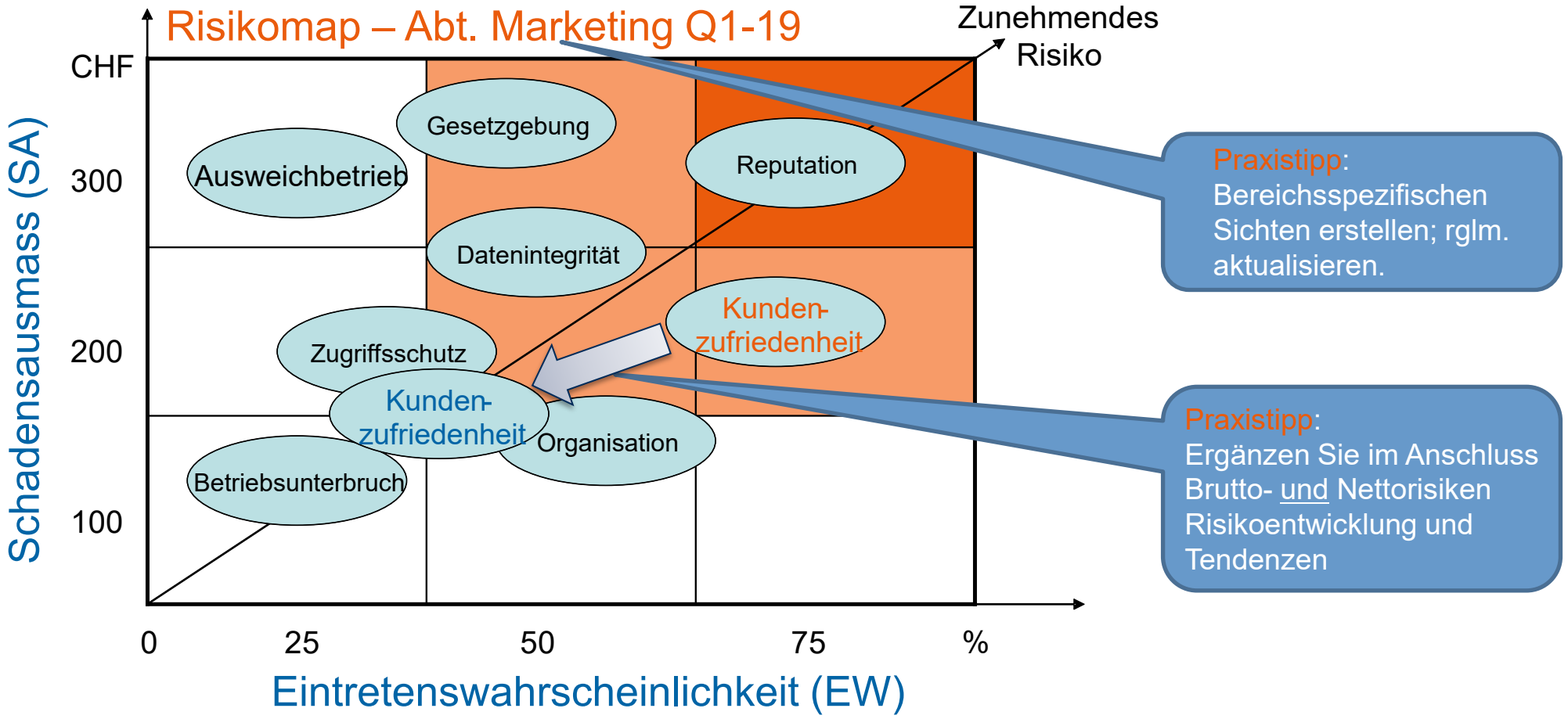
Methoden zur Bewertung des Risikoausmasses:

- Wahrscheinlichkeitsverteilungen
- Sensitivitäten / Stresstests und Szenarien

Praxistipp: Tabellen zum SA sollten je Bereich getrennt erstellt werden. Das gleiche Risiko kann auf Konzernstufe unbedeutend sein, bei einer Beteiligung jedoch bestandsgefährdend.

Risikomatrix mit Brutto und Nettorisiko

Grafische Umsetzung des Risiko-Katalogs



Internes Kontrollsystem
Bereichsspezifische - Risiko-Kontroll-Matrix

Bereichsziel

Teilprozesse/ Teilprozessziele		Risikoanalyse: Risikofaktoren/ Risikobeschreibung	Risikoanalyse: Rating	Steuerungs- und Kontrollmassnahmen: Kontrolle / Massnahmen/ Kommentare	Steuerungs- und Kontrollmassnahmen: Verantwortliche(r)	Steuerungs- und Kontrollmassnahmen: Typ (manuell/ automatisch; präventiv/ detektiv)	Beurteilung/ Schlussfolgerung (ok/nein, Kommentar)
Bestellung							
Bestellungen werden korrekt durchgeführt.	1	Bestellungen sind nicht geschäftsmässig begründet.	gering	Es erfolgt eine genaue Überprüfung durch eine dritte Person.	vom Einkaufsleiter unabhängige Person	m, p	ok
	2	Falsche Bestellungen werden aufgegeben (z.B. Waren/Dienstleistungen, die nicht benötigt werden).	hoch	• Bestellungen werden nur nach entsprechender Bestellanforderung aufgegeben. • Bestellungen werden vom Verkaufsleiter genehmigt und mit Bestellanforderung oder Kundenauftragskopie abgeglichen. • Bestellungen können nur von Einkäufern in das System eingegeben werden. • Nur Einkaufsleiter und dasjenige Personal, das die Bestellung angelegt hat, können die Bestellung ändern.	Einkäufer, Einkaufsleiter	m, d	ok
	3	Trotz Bestellanforderungen werden Waren nicht bestellt, oder Bestellanforderungen gehen verloren.	gering	• Bestellanforderungen und Bestellungen sind durchnummeriert. • Regelmässig wird überprüft, ob alle Bestellanforderungen und Bestellungen im System erfasst wurden (anhand der Nummern). • System gibt regelmässig automatisch eine Liste von nicht verwendeten (übersprungenen) Nummern aus, die überprüft werden.	Einkäufer	m/a, p/d	ok

1. Prozessziele → 2. Risiken → 3. Kontrollmassnahmen/Verantwortlichkeiten/Termine → 4. Audit

Die Risiko-Kontroll-Matrix ist Teil des int. Risk-Framework COSO

Entwicklung COSO

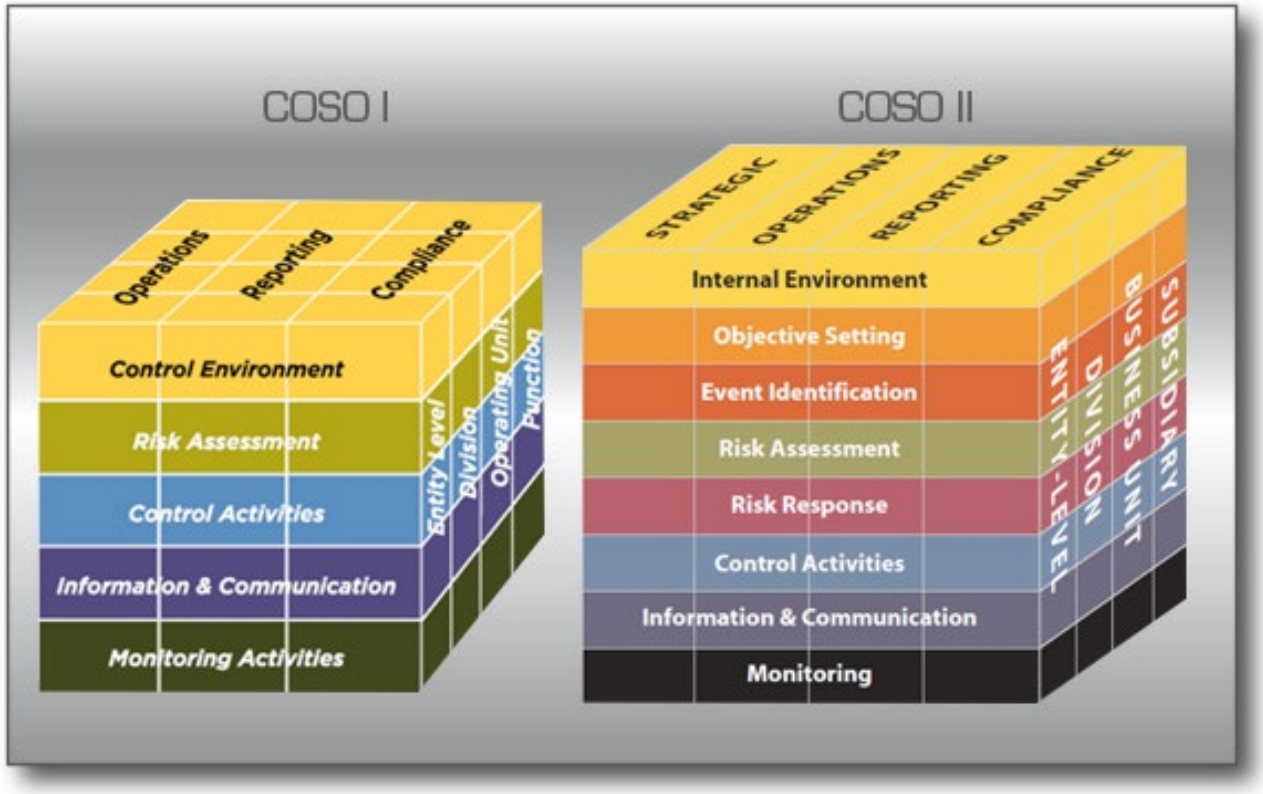
1985 – Gründung COSO

1992 – Veröffentlichung Internal Control Framework

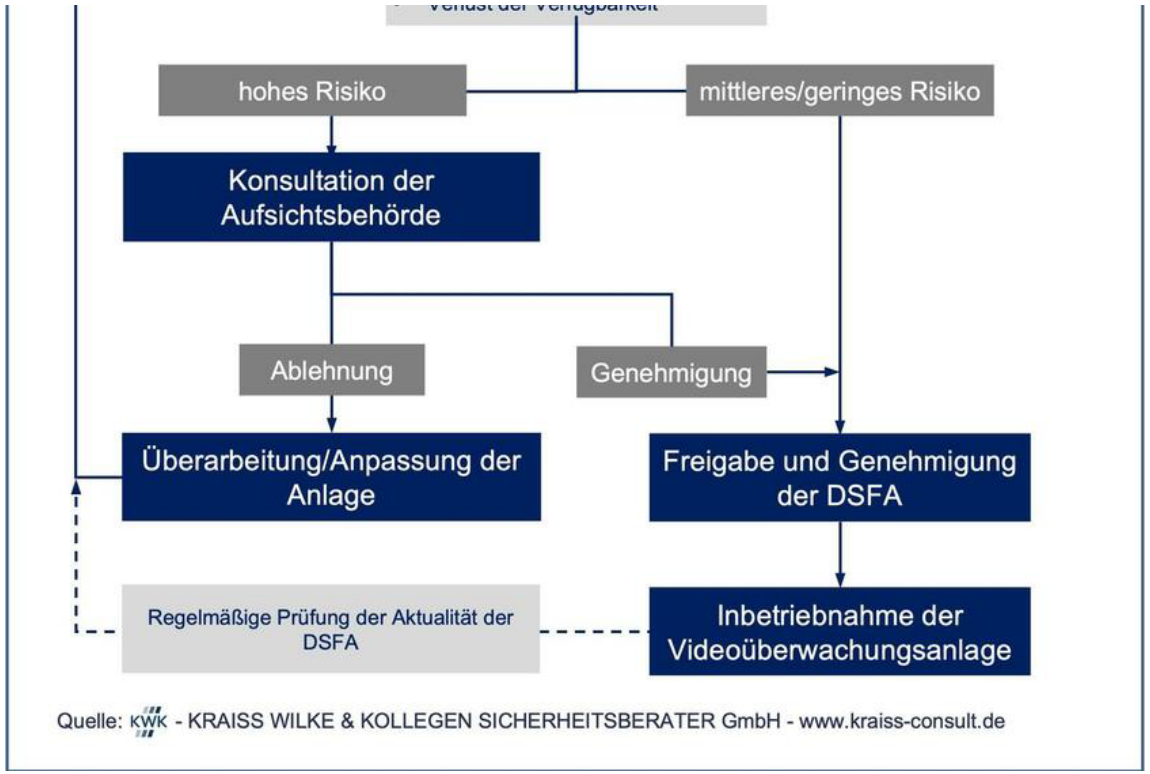
2002 – Anerkennung für SOX

2004 – COSO ERM (COSO II)

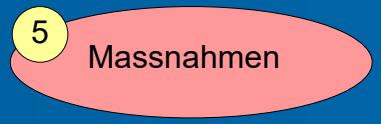
2013 – Weiterentwicklung von COSO II



Beispiel einer Risikobeurteilung im Datenschutz, die Datenschutz-Folgeabschätzung Art. 35 DSGVO bzw. Art. 22 revDSG



Risikomanagement
Wie geht Risikosteuerung



Risikosteuerung

- Dies ist die (kontinuierliche) Massnahmenplanung,
- deren Umsetzungskontrolle,
- um angemessen auf Störereignisse und künftige Risiken reagieren zu können.

Die identifizierten und überwachten Risiken werden **EINER oder MEHRER** möglichen Risikobegegnungsstrategien zugewiesen

Risikobegegnungsstrategien

- **Vermeiden** (Unterlassen von Aktivitäten)
- **Vermindern/Vorbeugen** (Schutz- und Sicherungsmassnahmen)
- **Transfer** (z.B. Versicherung oder Überwälzen der Risiken auf Dritte)
- **Akzeptanz** (und Frühwarnsystem)

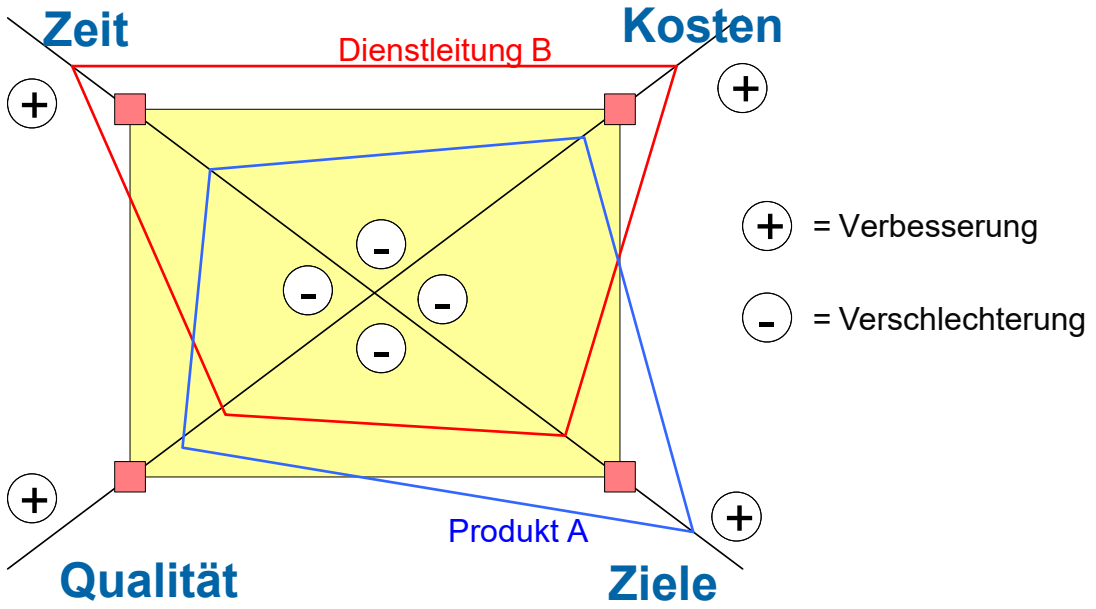
Risikomanagement
Dilemma im Risikomanagement

Konflikte ergeben sich aus vier unterschiedlichen Zielparametern:

- **Ziele** (Global-, Bereichs- und Teilziele) mit den vorgesehenen
- **Kosten** innerhalb der vorgesehenen
- **Zeit** in der geforderten
- **Qualität** (Datensicherheit..)

Fazit:

Die **Ressourcen für risikoreduzierende Massnahmen** sind **begrenzt**.



Agenda

- Cases-Behörden-Gerichtsentscheide
- Vorgaben und Regulierung zum Risiko
- Risikobegriff – in Ökonomie und Recht
- Risikomanagement und Audit Risiko
- Fazit

Beim Risikomanagement ist das «Audit» Risiko einzubeziehen

RISIKEN DER ENTDECKUNG

Audit-Risiko

INHERENT RISK

Risiken aus dem Geschäftsfeld, der Daten, Quantität, ext. Einflüsse, etc.

VERSAGEN DER RISIKOKONTROLLE

Kontrollmassnahmen zur Früherkennung könne versagen

AUFSPÜREN VON RISIKEN

Risiko, dass Abweichungen nicht erkannt werden.

Agenda

- Cases-Behörden-Gerichtsentscheide
- Vorgaben und Regulierung zum Risiko
- Risikobegriff – in Ökonomie und Recht
- Risikomanagement und Audit Risiko
- Fazit

Fazit zum Risikomanagement in Recht und Praxis

- ✓ Risiko gehört zu jedem wirtschaftlichen handeln
- ✓ Business Judgement Rule gibt Sicherheit unter der Vorgabe sorgfältiger Abwägung
- ✓ Das Risiko wir in einem strukturierten Prozess ermittelt
- ✓ Massnahmen zur Risikosteuerung sind zu dokumentieren und überwachen
- ✓ Kontrollen sorgen für einen frühe Erkennung bei Abweichungen
- ✓ Eingebettet ist das Risikomanagement in grossen Unternehmen im Unternehmens – IKS
- ✓ Die Datenschutzfolgeabschätzung ist Teil des gesamt Risikomanagement-Prozesses
- ✓ Das Auditrisiko beschreibt die Unsicherheit dass schlagende Risiken erkannt werden.

Vielen Dank.

März 2023