~~Risikomanagement~~

Management un-gewisser Un-Werte

im Mittelstand nach standardisierten Praktiken (von ISO bis COSO)

11.04.2019 / Dresden - Mittelstandstag 2019 -
Hochschule Technik und Wirtschaft

Dr. Peter Meier, Steinbeis Transferzentrum Risikomanagement

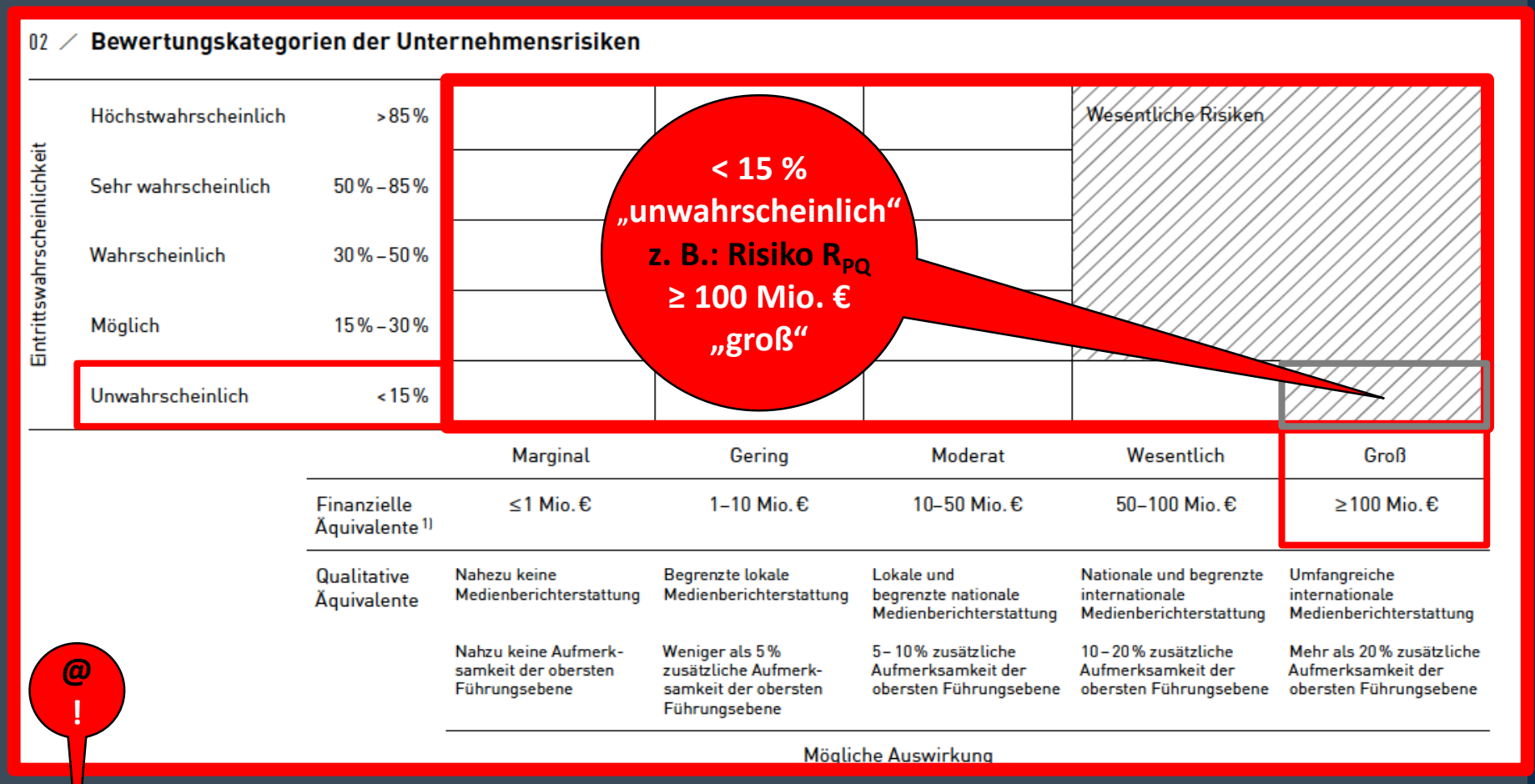
https://risikoundchance.blogspot.com/
peter.meier@steinbeis.de

10 Kurzgeschichten (Auswahl des Autors)

1. Qualitätsrisiken?	aus der Praxis / Beispiel adidas AG / Anwendung KMU
2. Denkdefizite Risikomatrix	aus der Praxis / Beispiel adidas AG / Anwendung KMU
3. Risikodefinitionen	dies- und jenseits der ISO / (un-) gewissen (Un-) Werte
4.a Ungewissheit	ein „Zustand“ des Wissens
4.b Wahrscheinlichkeit	eine bedingte mathematische „Kausalität“
5. Risiko Text-Aufgaben	Monte Carlo Zahlen-Lösungen
6. ISO 9001:2015	kein Risikomanagementsystem! / Anwendung KMU
7. ISO 31000:2018	kein Risikomanagementsystem! / Anwendung KMU
8. IDW (COSO) PS 981 (2017)	bezogen auf ein Wertesystem! / Anwendung KMU
9. Integration	Risikomanagement in / mit Wertemanagement in KMU
10. f osi 1001:1781	Norm: Managementsystem für (un-) gewisse (Un-) Werte

Literatur

Quelle: Adidas (KPMG) Jahresbericht 2014 Seite 156 *(Bildzitat)*
(zur Illustration der Praxis der „Risikomatrix“)



Hervorhebungen durch den Autor ***(vgl. IEC / ISO 31010:2009 B.29)***

1. Qualitätsrisiken ?

Steinbeis-Transferzentrum Risikomanagement

Quelle: Adidas (KPMG) Jahresbericht 2014 Seite 162 *(Bildzitat)*
(zur Illustration des Themas „Produktqualitätsrisiken“)

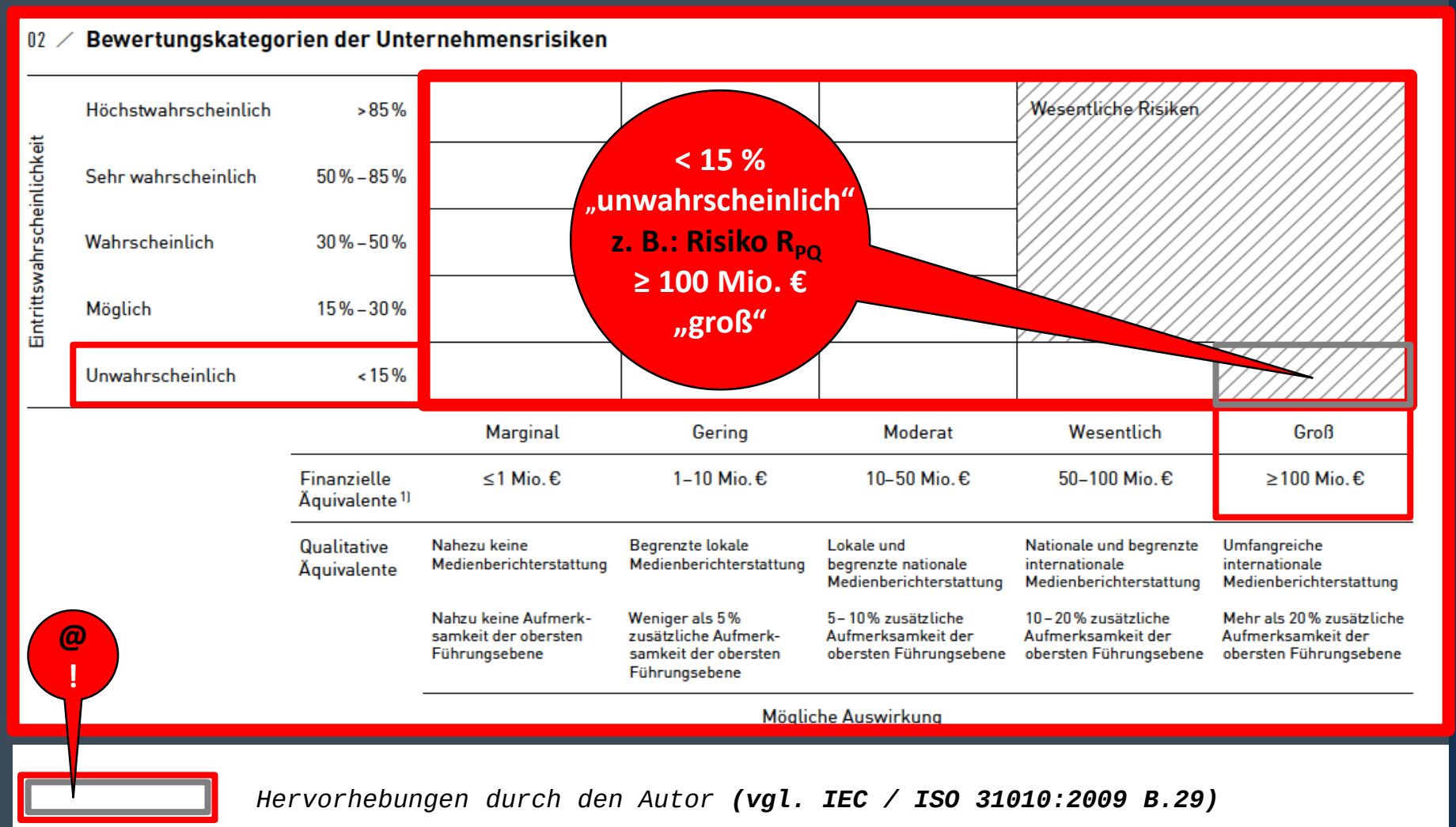
Rechtliche & Compliance-Risiken				
Risiken in Verbindung mit Wettbewerbs-, Handels-, Zoll- und Steuerbestimmungen	Groß		Unwahrscheinlich	↓ (Möglich)
Produktqualitätsrisiken	Groß	↑ (Wesentlich)	Unwahrscheinlich	↓ (Möglich)
Risiken von Betrug und Korruption	Groß		Unwahrscheinlich	
Risiken in Verbindung mit Produktfälschungen und -nachahmungen	Wesentlich		Wahrscheinlich	↑ (Unwahrscheinlich)

< 15 %
„unwahrscheinlich“
Risiko R_{PQ}
≥ 100 Mio. €
„groß“

@
!

Hervorhebungen durch den Autor ***(vgl. IDW PS 981:2017)***

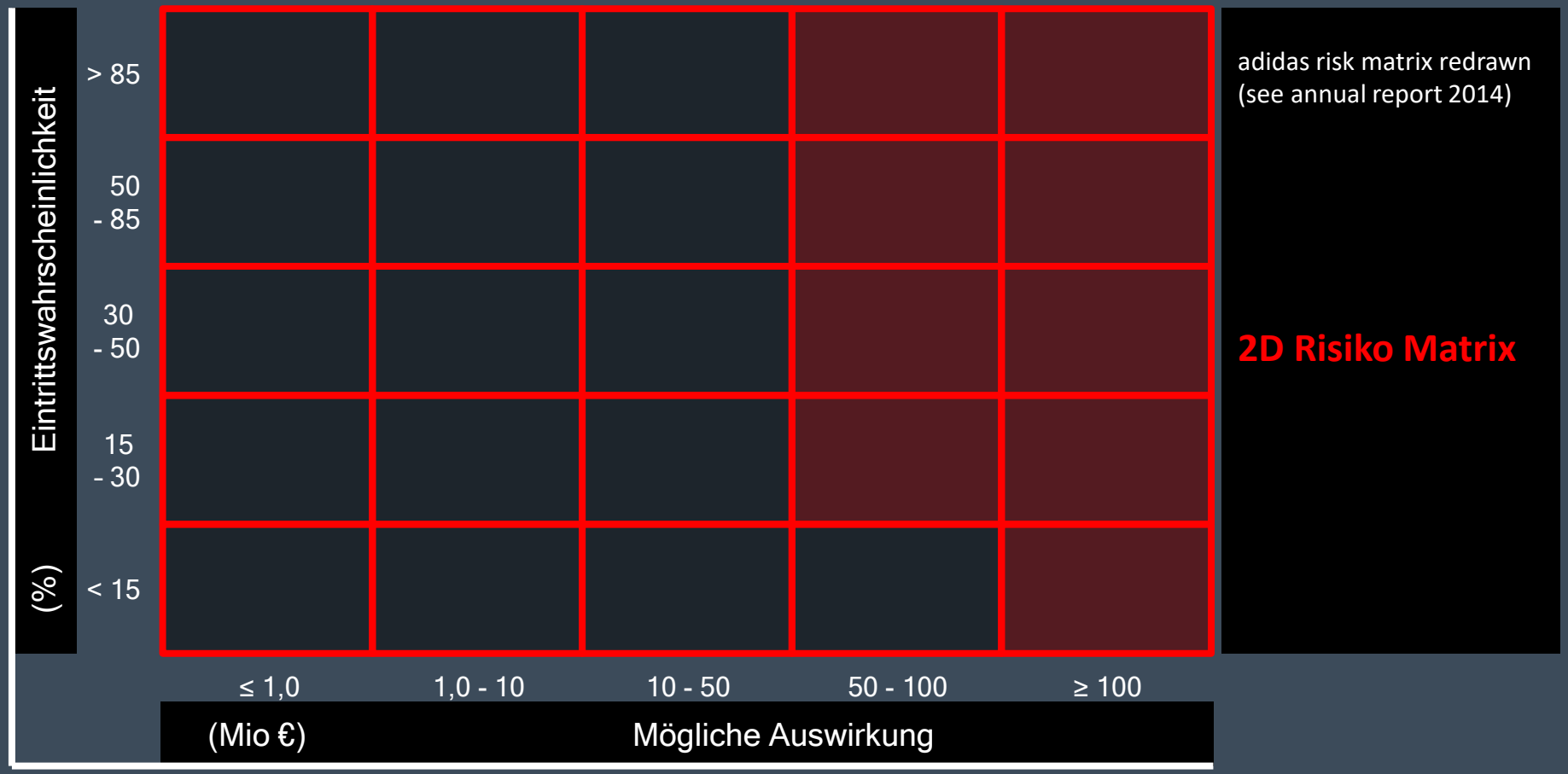
Quelle: Adidas (KPMG) Jahresbericht 2014 Seite 156 *(Bildzitat)*
(zur Illustration der Praxis der „Risikomatrix“)



Hervorhebungen durch den Autor ***(vgl. IEC / ISO 31010:2009 B.29)***

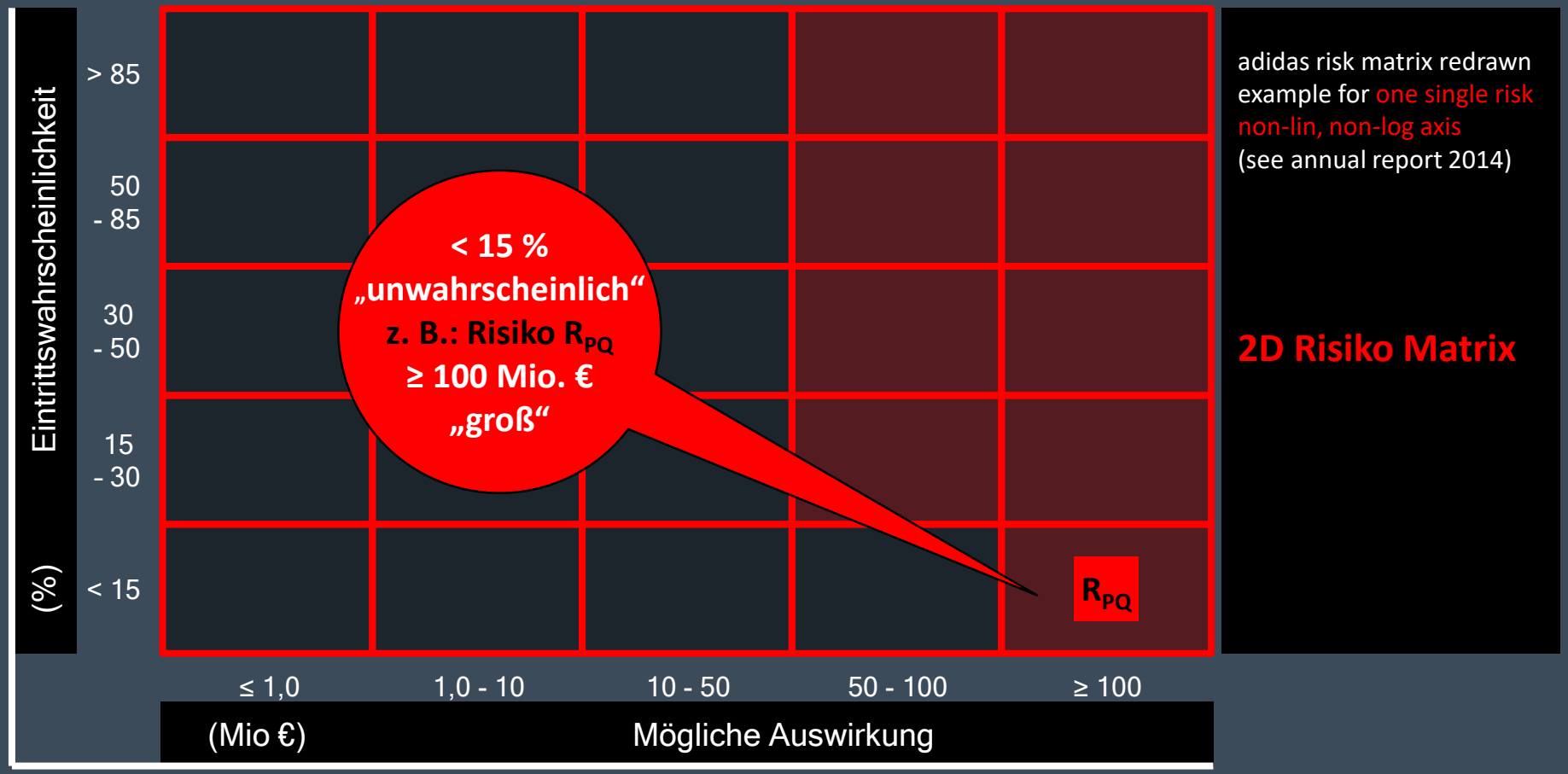
2. Denkdefizite Risikomatrix

Steinbeis-Transferzentrum Risikomanagement



2. Denkdefizite Risikomatrix

Steinbeis-Transferzentrum Risikomanagement

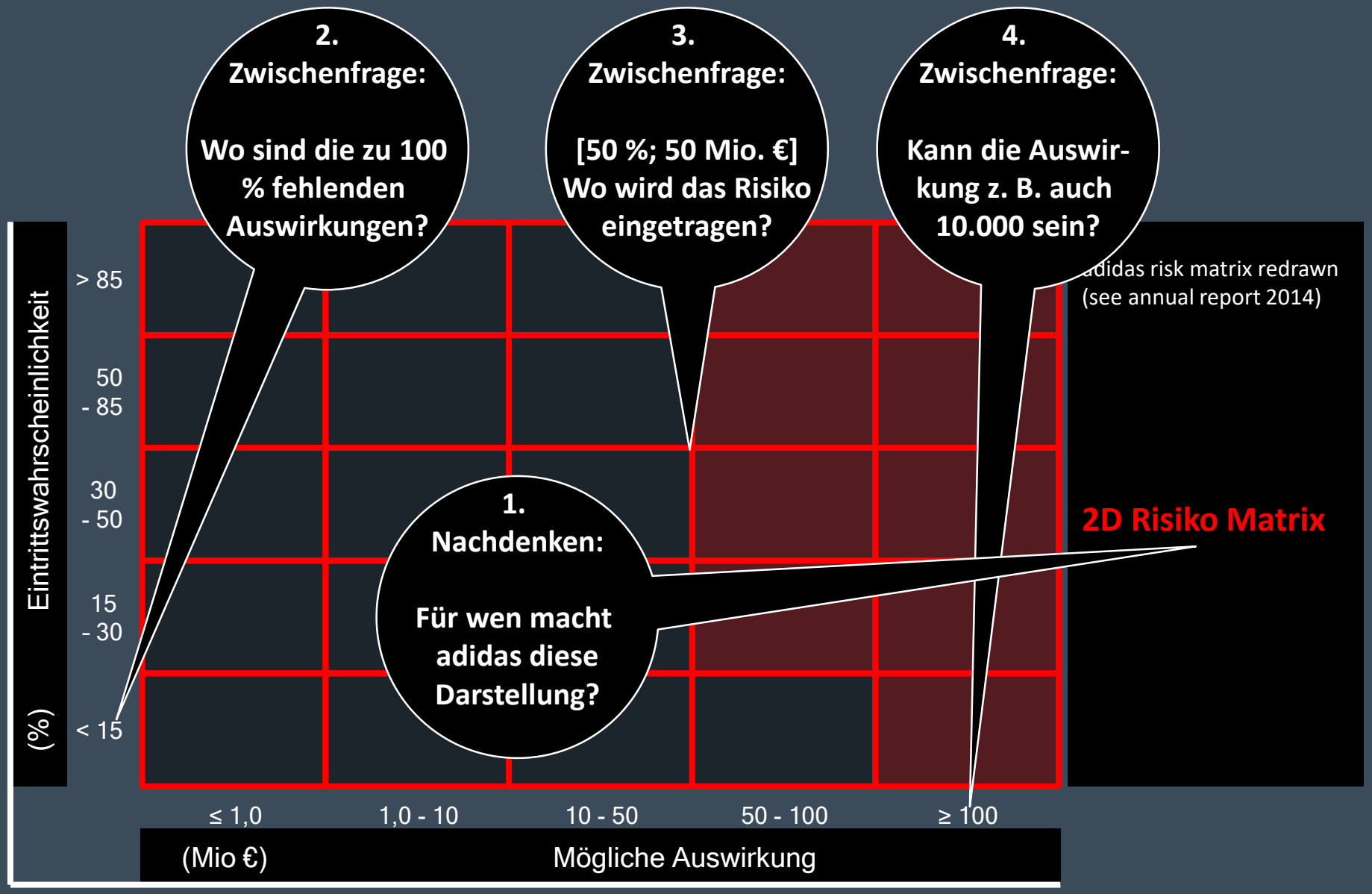


adidas risk matrix redrawn
example for one single risk
non-lin, non-log axis
(see annual report 2014)

2D Risiko Matrix

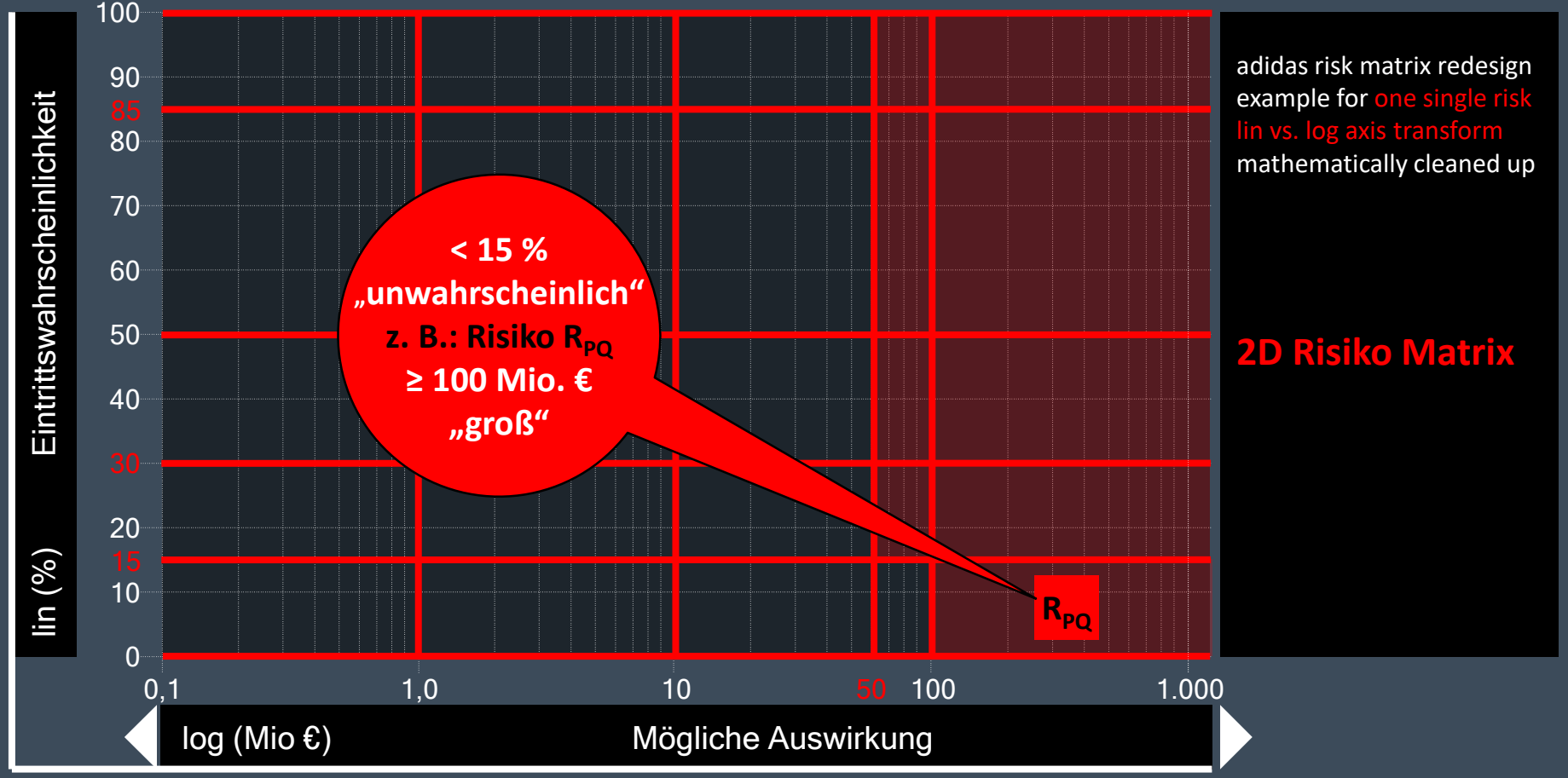
2. Denkdefizite Risikomatrix

Steinbeis-Transferzentrum Risikomanagement



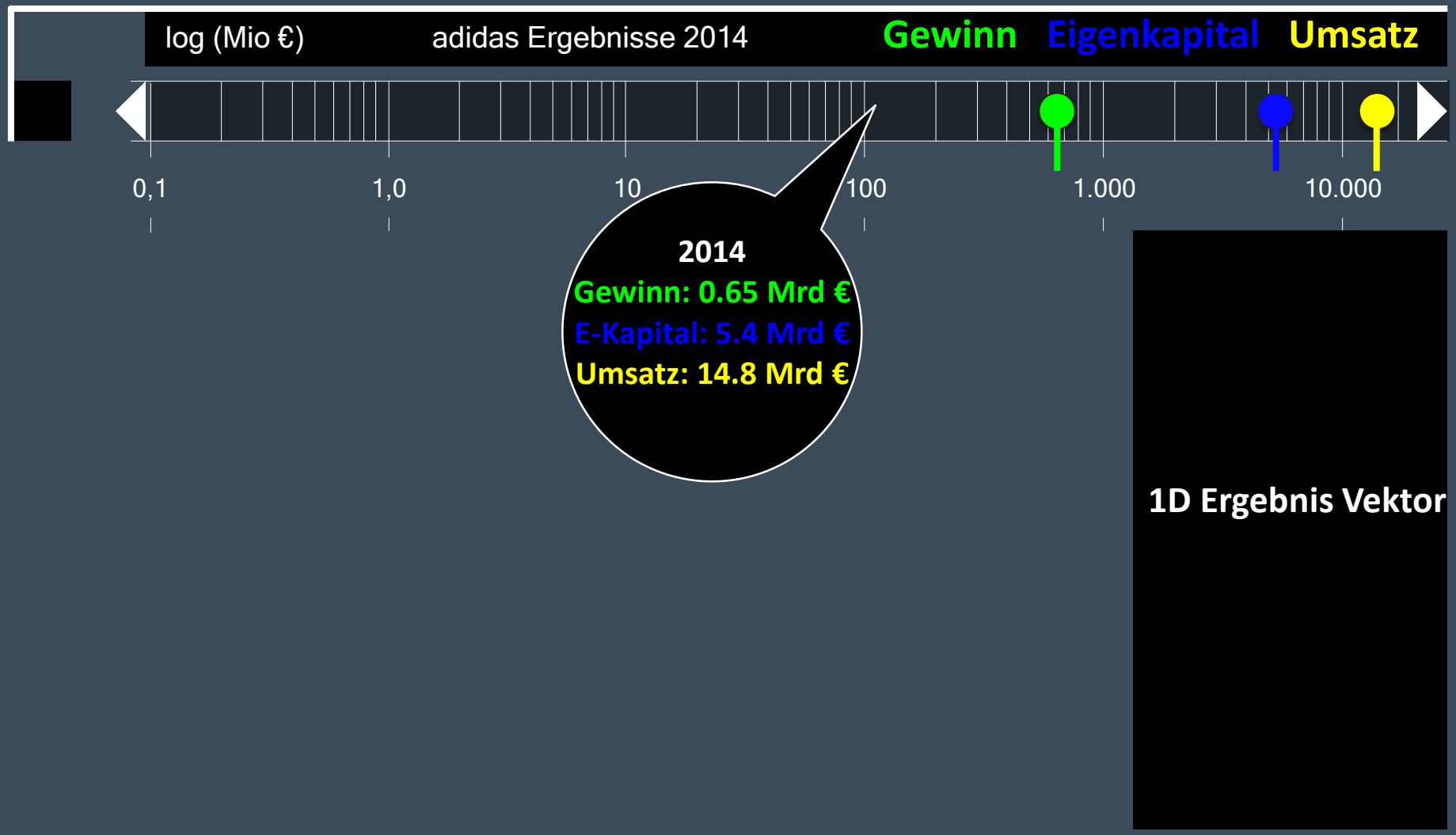
2. Denkdefizite Risikomatrix

Steinbeis-Transferzentrum Risikomanagement



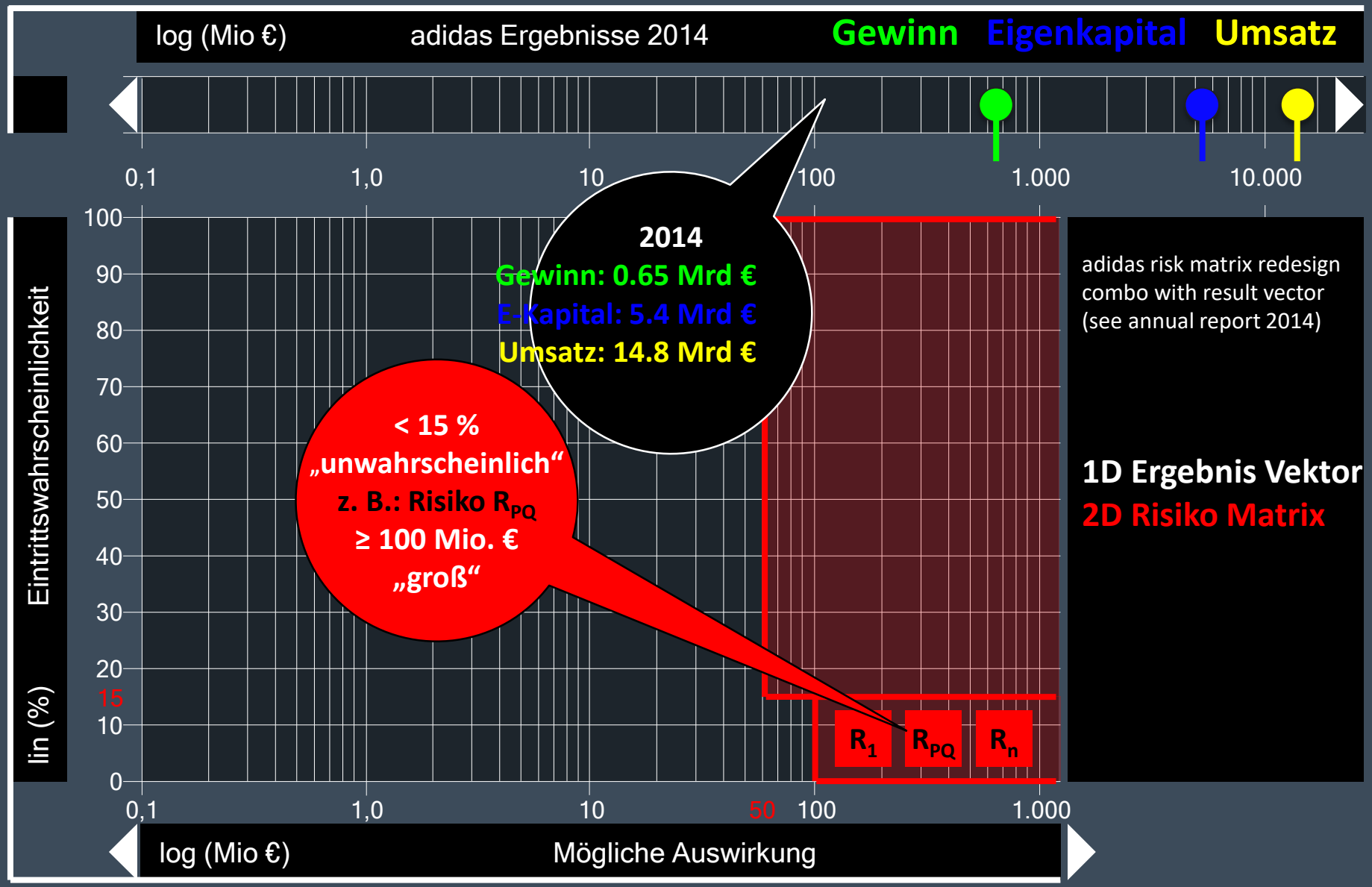
2. Denkdefizite Risikomatrix

Steinbeis-Transferzentrum Risikomanagement



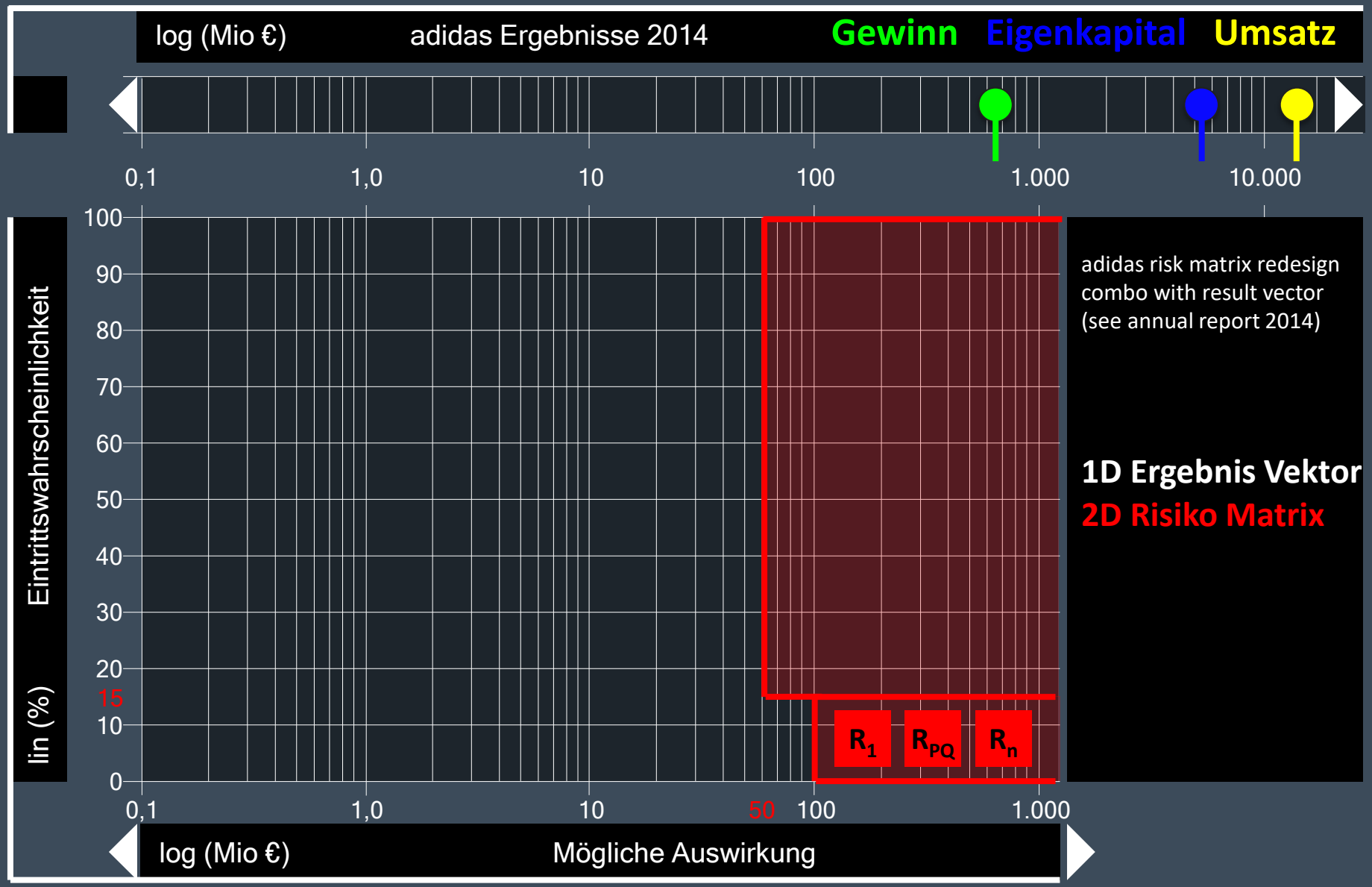
2. Denkdefizite Risikomatrix

Steinbeis-Transferzentrum Risikomanagement



2. Denkdefizite Risikomatrix

Steinbeis-Transferzentrum Risikomanagement



3. Risikodefinitionen

Steinbeis-Transferzentrum Risikomanagement

*DIN EN **ISO 9000:2015** Normabschnitt 3.7.9*
Risiko: „Wirkung von Ungewissheit“

*DIN EN **ISO 14001:2015** Normabschnitt 3.2.10*
Risiko: „Auswirkung von Ungewissheit“

*DIN EN **ISO 14001:2015** Normabschnitt 3.2.11*
Risiken und Chancen: „Potenziell ungünstige Auswirkungen (Bedrohungen) und potenziell günstige Auswirkungen (Chancen)“

*DIN **ISO 31000:2018** Normunterkapitel 2.1*
Risiko: „Wirkung von Ungewissheit auf Ziele“

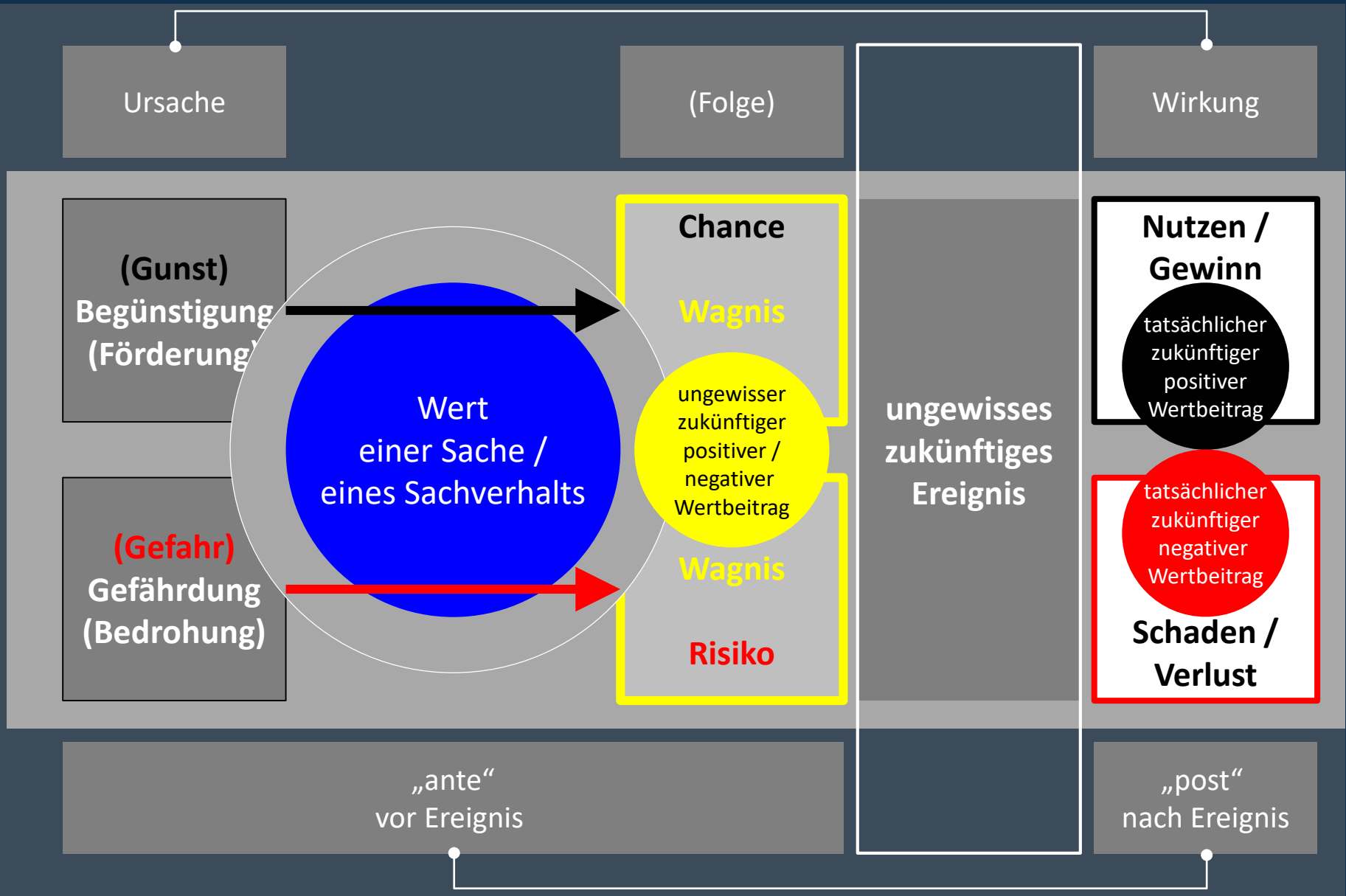
IDW PS 340
Risiko: „ ... allgemein die Möglichkeit ungünstiger künftiger Entwicklungen ... “

IDW PS 981:2017
Risiken: „ ... mögliche künftige Entwicklungen oder Ereignisse, die zu einer für das Unternehmen negativen (Risiko im engeren Sinne) oder positiven (Chance) Zielabweichung führen können.“

f osi 1001:1781
Risiko: „ ... ungewisse zukünftige negative Wertposition ... “

3. Risikodefinitionen

Steinbeis-Transferzentrum Risikomanagement



Risiko Wahrnehmung

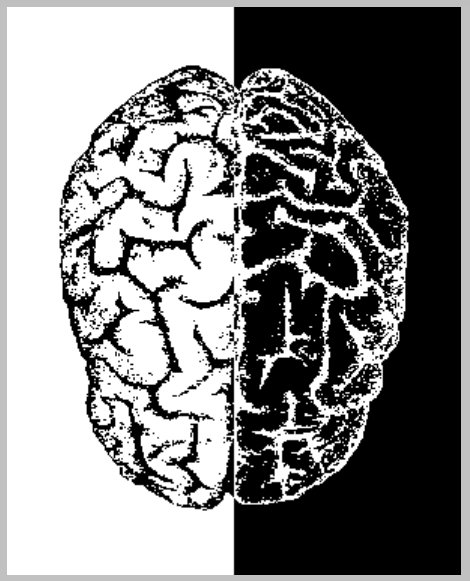
von der
- Ungewissheit (psychologisch)

zu der
- Wahrscheinlichkeit (mathematisch)

„Rechtshirn“

Gefühl
Instinkt
Intuition
Reflex
Erfahrung

Emotio

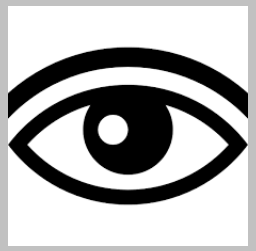


„Linkshirn“

Verstand
Intellekt
Logik
Mathematik
Wissen

Ratio

Ungewissheit



Wahrscheinlichkeit

„Ungewissheit“ *(Übersetzung)*
„Wahrscheinlichkeit“?

Textbeispiele:

1. Wie groß ist ein Risiko?

1. Wie lange dauert es (**Prognose**), bis ein Projekt mit 95 % Wahrscheinlichkeit / Sicherheit entsprechend der Ziele abgeschlossen ist?

2. Quantitative Beurteilung der **Redundanz** in Infrastrukturen: (Energie, Material, Information, ...)

3. **value@risk** für nicht-finanzielle Wertesysteme: Wieviel Reputation büße ich „möglicherweise“ ein?

Beispiel zu 2. aus 2012
Termin- / Zeitrisiko
(veröffentlicht)

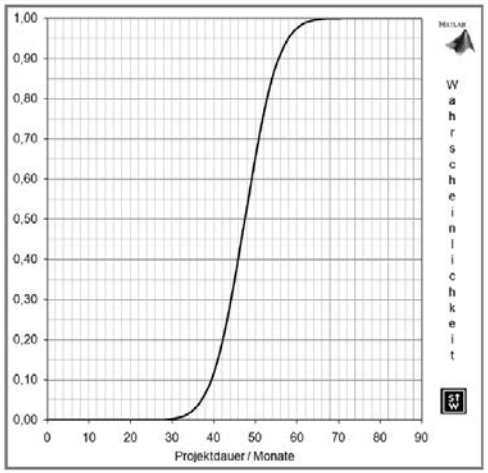


Abbildung 1. Zeitlicher Verlauf der Sicherheit eines Projektabschlusses aus einer typischen Monte-Carlo Simulation.

Chemie Ingenieur Technik

Essay

Risikomanagement in Großprojekten

Peter Meier

DOI: 10.1002/cite.201100182

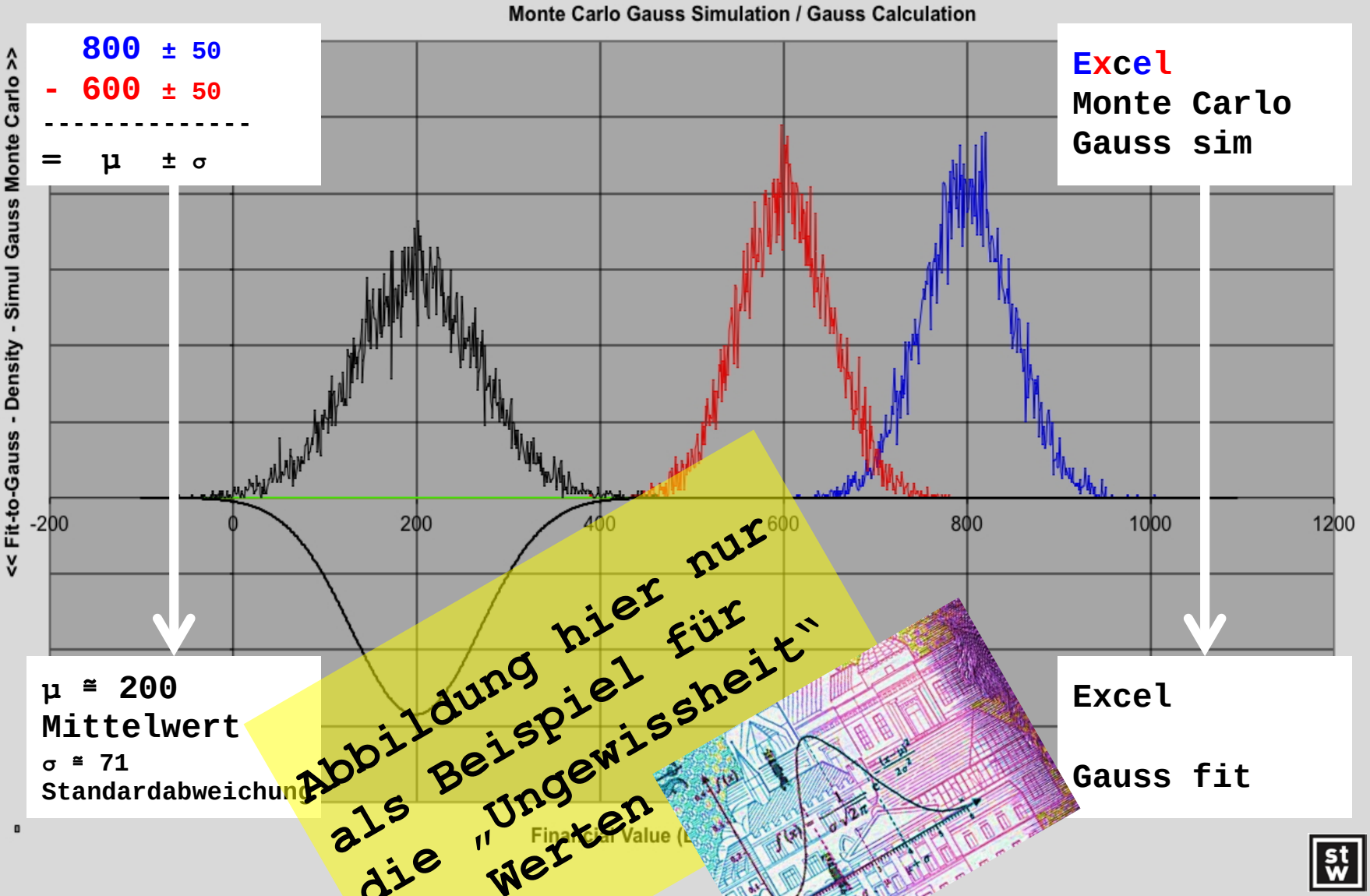
Herrn Prof. Dr. Klaus Müller († 2011), Universitá degli Studi di Trento, gewidmet

Industrielle Großprojekte sind mit beträchtlichen technischen und unternehmerischen Risiken verknüpft. Das Projektmanagement schließt ein Risikomanagement mit ein. Die Beurteilung der Risiken ist Teil der Entscheidungen in allen Phasen des Projekts. Das Risikomanagement in Projekten ist weitgehend standardisiert und bedient sich stochastischer Planungsmodelle, die mit Monte-Carlo Rechnungen simuliert werden.

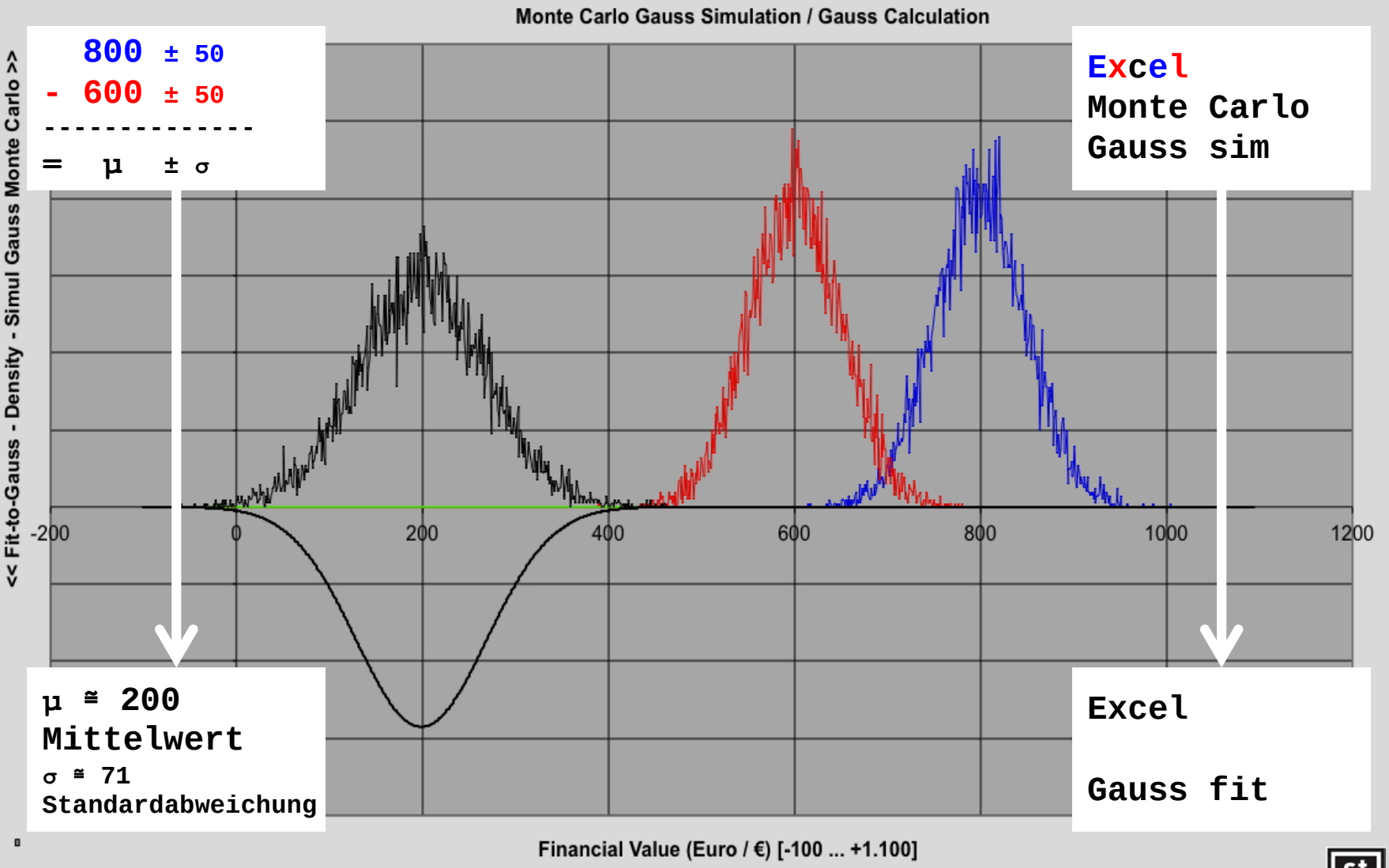
Schlagwörter: Großprojekte, Internationale Normen, Projektmanagement, Projektrisiken, Risikomanagement

Eingegangen: 12. Oktober 2011; *akzeptiert:* 17. Februar 2012

Steinbeis-Transferzentrum Risikomanagement



Steinbeis-Transferzentrum Risikomanagement



800 ± 50
- 600 ± 50

= μ ± σ

Excel
Monte Carlo
Gauss sim

μ ≅ 200
Mittelwert
σ ≅ 71
Standardabweichung

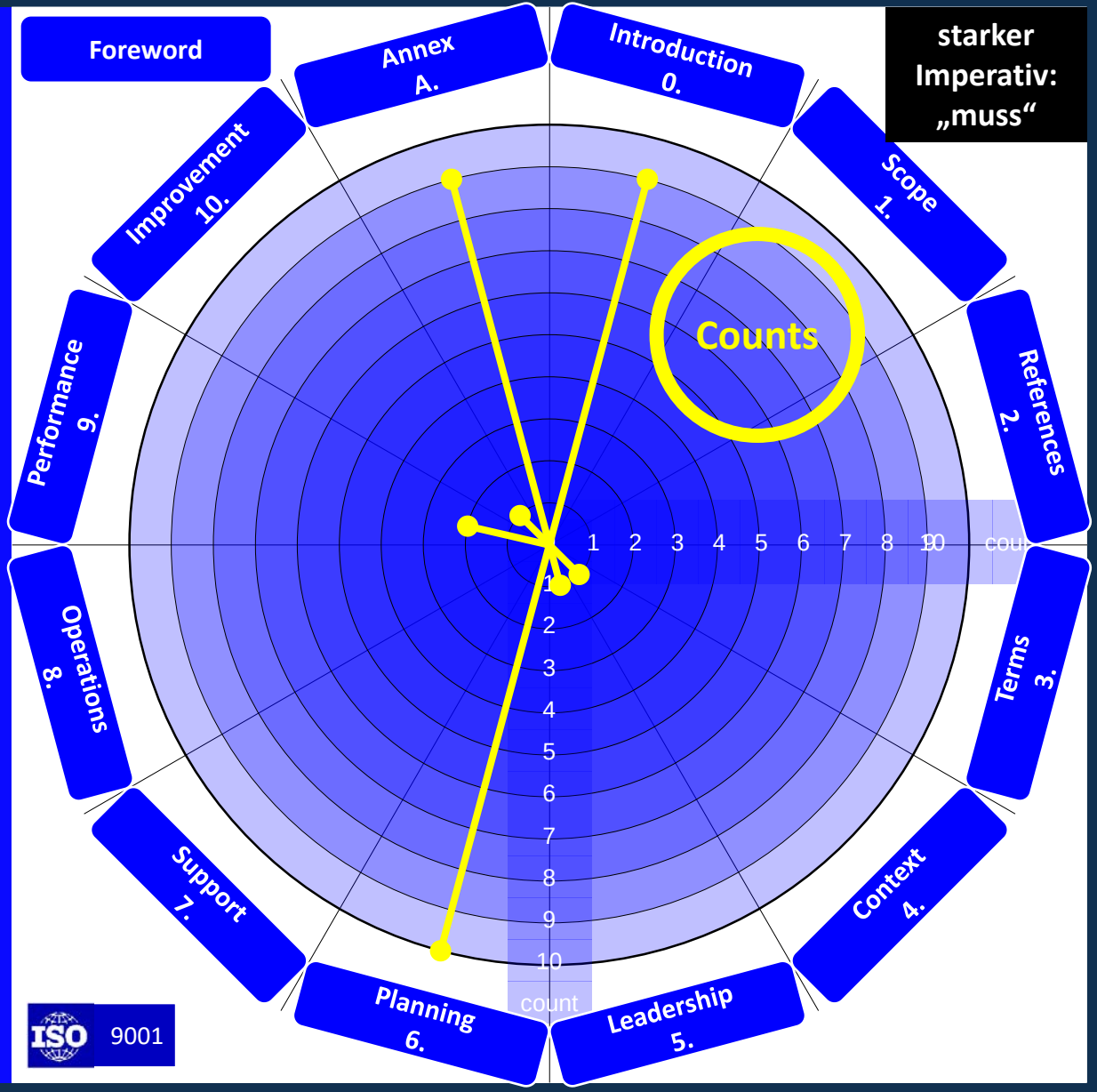
Excel

Gauss fit

Steinbeis-Transferzentrum Risikomanagement

„risk“ ISO 9001:2015		
Chapter	Count	Requirements
0.	9	-
1.	0	-
2.	0	-
3.	0	
4.	1	1
5.	1	1
6.	10	3
7.	0	0
8.	0	0
9.	2	2
10.	1	1
A.	9	-

DIN EN ISO 9001:2015
Qualitätsmanagement-systeme - Anforderungen

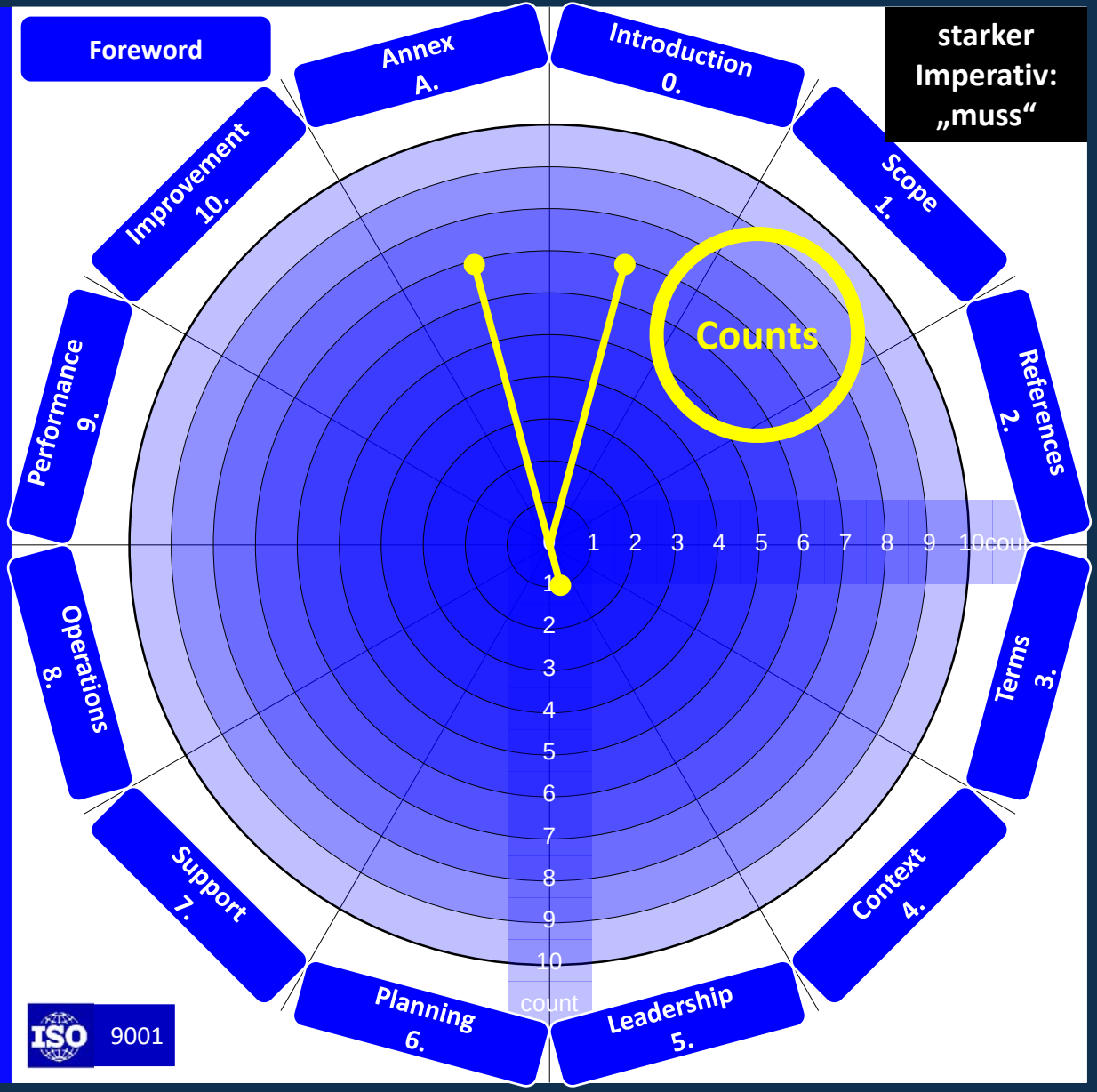


6. ISO 9001:2015

Steinbeis-Transferzentrum Risikomanagement

„risk based thinking“ ISO 9001:2015		
Chapter	Count	Requirements
0.	7	-
1.	0	-
2.	0	-
3.	0	
4.	0	0
5.	1	1
6.	0	0
7.	0	0
8.	0	0
9.	0	0
10.	0	0
A.	7	-

DIN EN ISO 9001:2015
Qualitätsmanagement-systeme - Anforderungen



Steinbeis-Transferzentrum Risikomanagement

Zitat: DIN EN ISO 9001:2015 Anhang A.4 Risikobasiertes Denken
(zur Illustration des Themas „Risiken - ISO 9001“)

ISO 9001

Relativierung des starken Imperativs „muss“ durch „obwohl“

Obwohl in 6.1 festgelegt ist, dass die Organisation Maßnahmen zur Behandlung von Risiken planen muss, sind keine formellen Methoden für das Risikomanagement oder ein dokumentierter Risikomanagementprozess erforderlich. Organisationen können entscheiden, ob sie eine ausgedehntere Vorgehensweise für das Risikomanagement, als von dieser Internationalen Norm gefordert wird, entwickeln möchten oder nicht, z. B. durch die Anwendung anderer Leitlinien oder Normen.

Hervorhebung durch den Autor

Steinbeis-Transferzentrum Risikomanagement

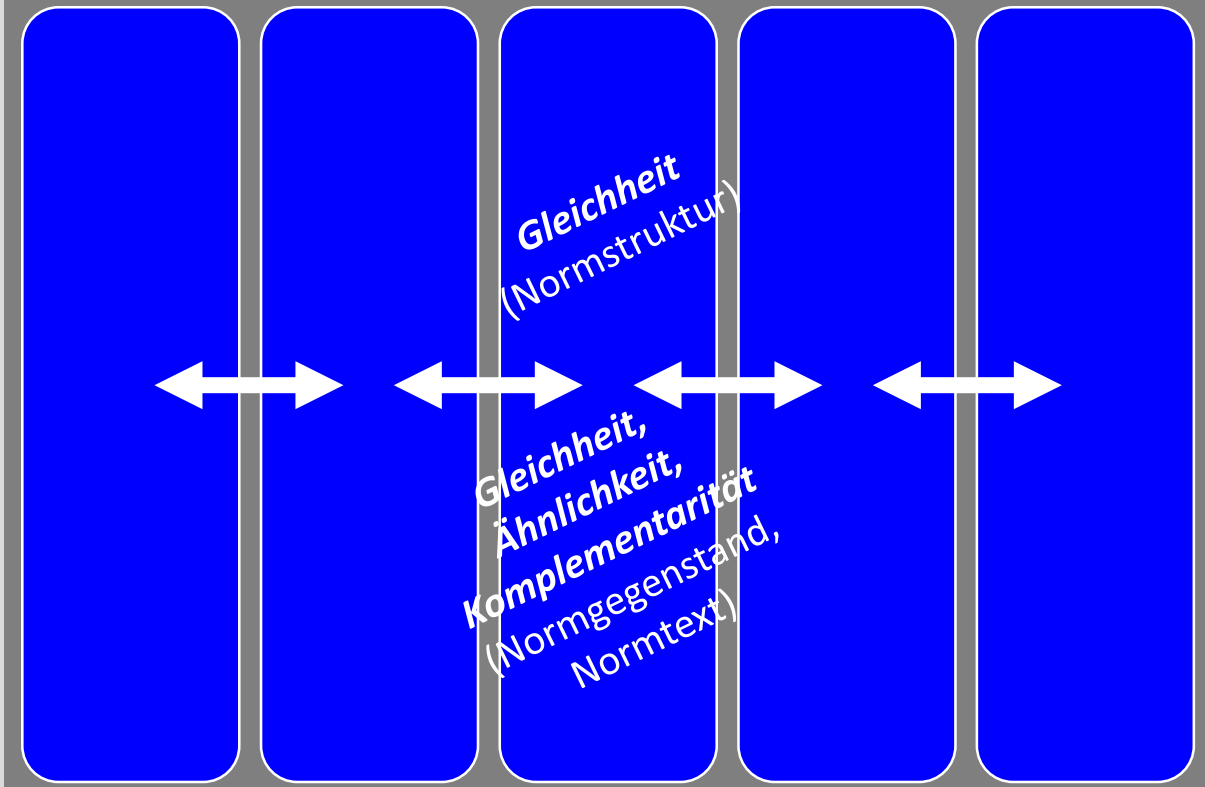
Titel:	ISO Themen Normen mit Anforderungen an Managementsysteme				
ISO Normen:	ISO 9001	ISO 14001	ISO 27001	ISO 45001	ISO XY001
ISO Themen: = Werte	(a) Qualität	(b) Umwelt	(c) Sicherheit	(d) Sicherheit	(e) andere

Ordnung von Werten in vertikalen „Silos“ nach ISO Themen Normen:
Silo (a) bis Silo (e) usw.

Nach den ISO Normen mit Anforderungen an Managementsysteme

Silo = horizontal differenziertes Managementsystem

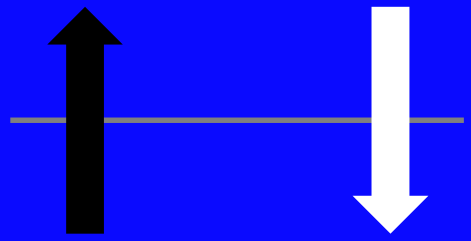
- **ISO-Silo-siert**
- **Silo-ISO-liert**



Steinbeis-Transferzentrum Risikomanagement

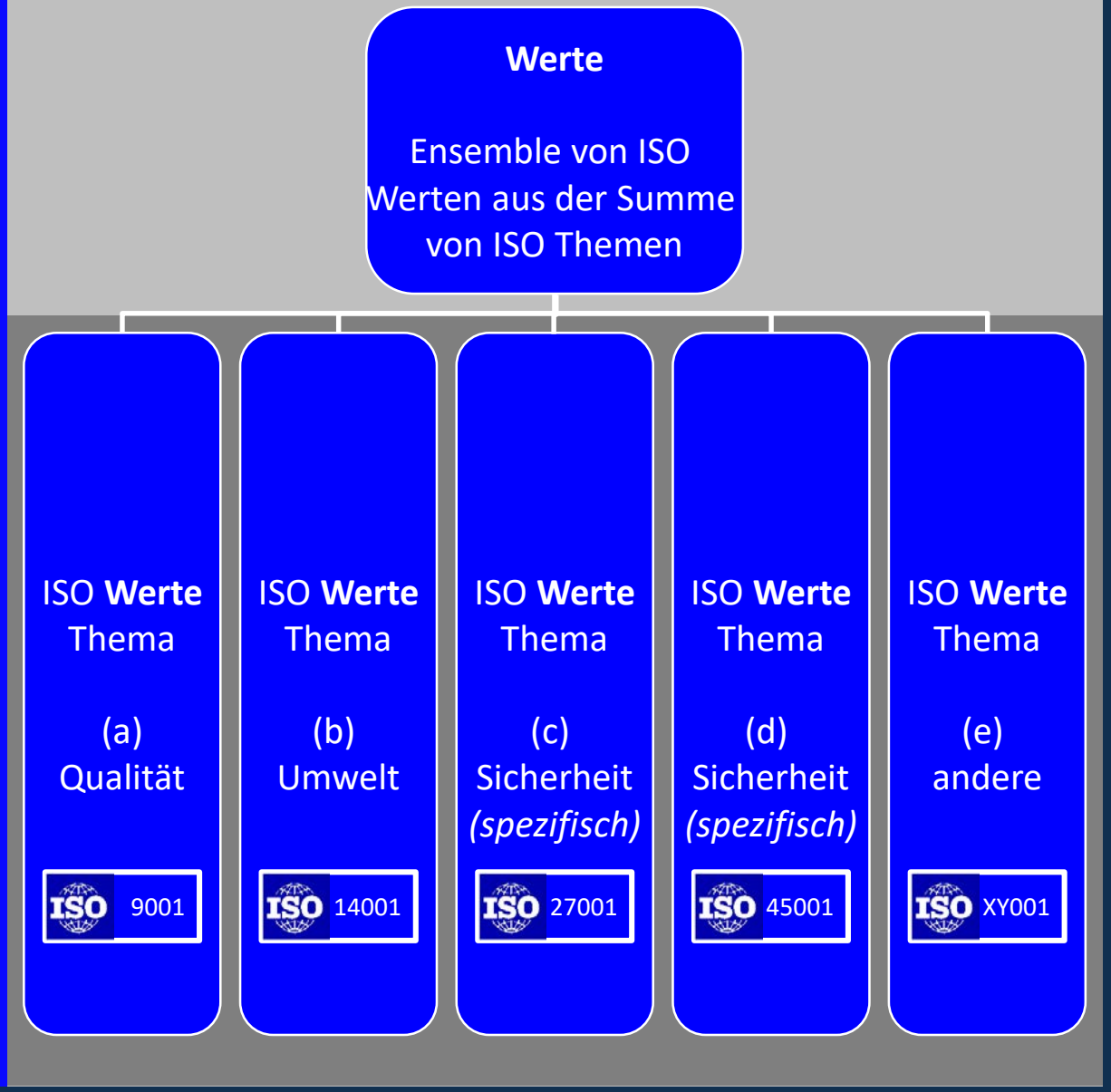
Management

- Integriert über Werte Themen



- Differenziert nach Werte Themen

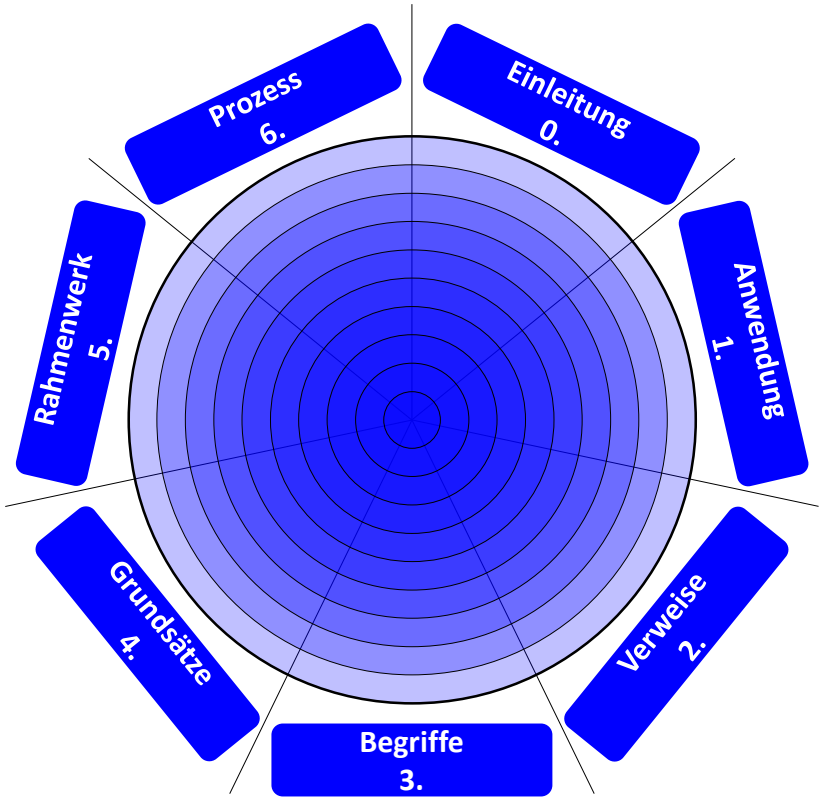
Management



- Keine 10 Kapitel MMS Struktur
- Bezug zu Werten in 0.
- Keine Anforderungen („muss“)
- Leitlinien = Empfehlungen („sollte“)
- Keine explizite Festlegung des Anwendungsbereichs
- Begriffswiki in 3.
- Kein expliziter Bezug zu MMS Standards
- Empfehlungen zu Integration in die Organisation in 5.
- PDCA-Zyklus versteckt in 5.
- Quasi-System in 5.
- Hinweise auf Gesamtorganisation in 5.
- Explizite Prozessbeschreibung in 6.

DIN ISO 31000:2018 Risikomanagement - Leitlinien

schwacher Imperativ: „sollte“



ISO 31000

8. IDW (COSO) PS 981 (2017)

Steinbeis-Transferzentrum Risikomanagement

:Titel

:IDW Standard

:COSO Kategorien = **Werte** *(erweitert)*

Ordnung von Werten in horizontalen „Ebenen“ nach COSO Kategorien (erweitert pm / Steinbeis): Ebene (1) bis (5)

Angelehnt an COSO Kategorien aus dem PS 981 des IDW

Ebene = vertikal differenziertes Managementsystem

Werte nach IDW (COSO) Kategorien

IDW PS 981

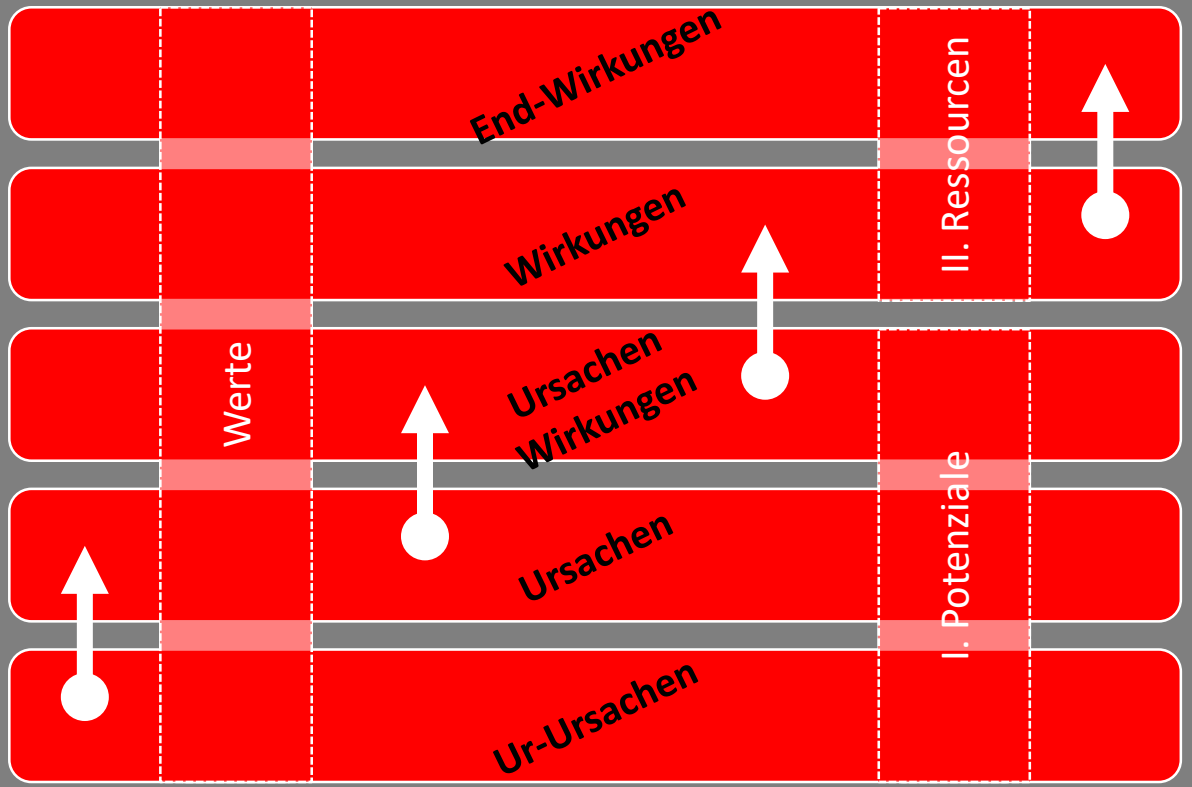
(5) finanziell **Budget**

(4) operativ **Betrieb**

(3) strategisch **Konzept**

(2) regulativ **Compliance**

(1) normativ **Governance**



8. IDW (COSO) PS 981 (2017)

Steinbeis-Transferzentrum Risikomanagement

Management
- Integriert über Werte Kategorien

- Differenziert nach Werte Kategorien

Management

Werte

Gesamtheit aller Werte als Summe der COSO Werte Kategorien *(erweitert)*

COSO **Werte** Kategorie	(5) finanziell **Budget**
COSO **Werte** Kategorie	(4) operativ **Betrieb**
COSO **Werte** Kategorie	(3) strategisch **Konzept**
COSO **Werte** Kategorie	(2) regulativ **Compliance**
COSO **Werte** Kategorie	(1) normativ **Governance**

Steinbeis-Transferzentrum Risikomanagement

Integration

von Werte- bzw. Risikomanagement für die Werte
(α) **Governance**
(β) **Compliance**
sowie für weitere **Werte**.

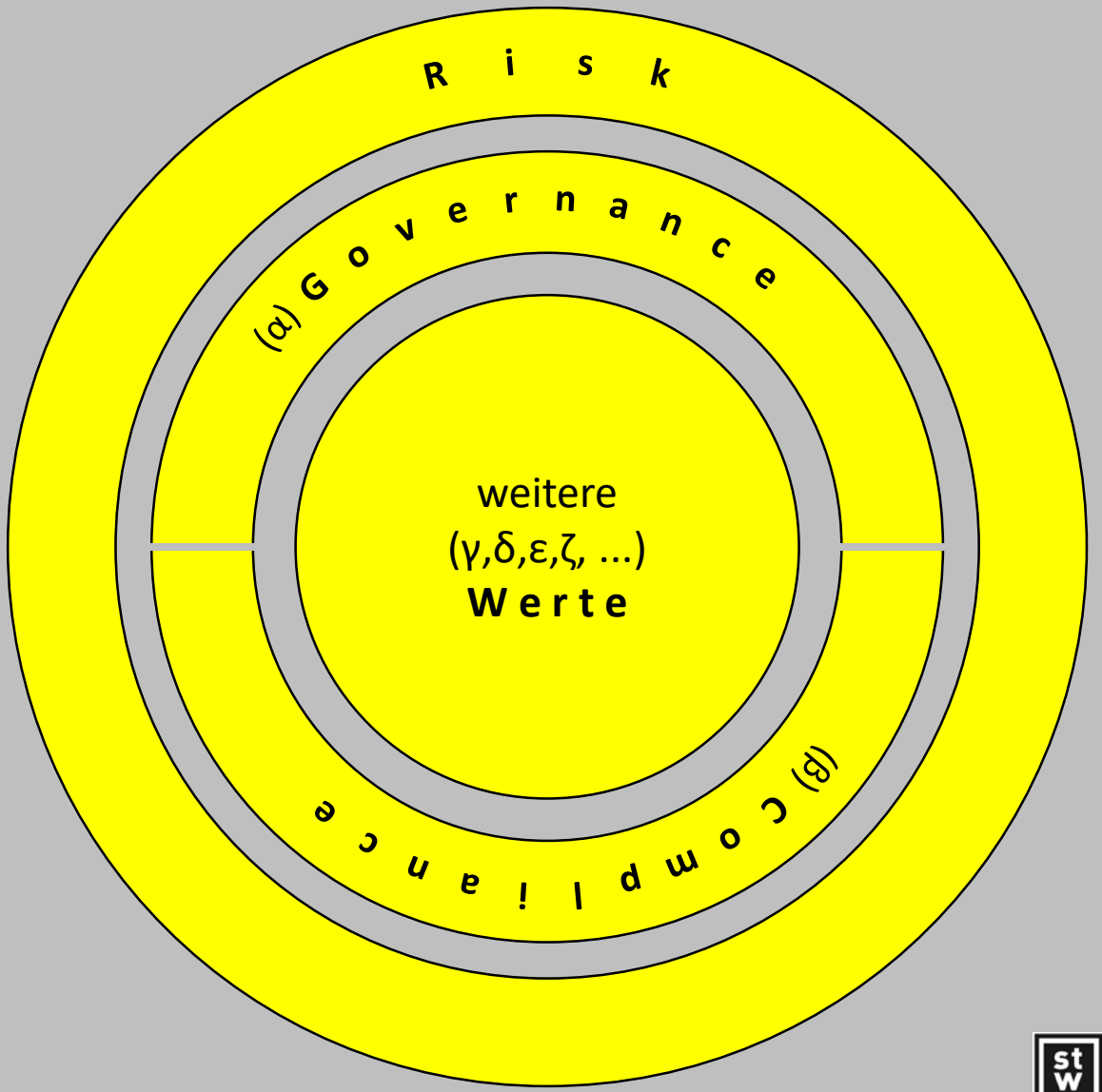
Das Management von **Werten** unterliegt den Bedingungen von

- **Governance**
- **Compliance**

die selbst **Werte** sind.
Alle Werte werden aus der Perspektive

- **Risk / Risiko**

gemanagt.



Steinbeis-Transferzentrum Risikomanagement

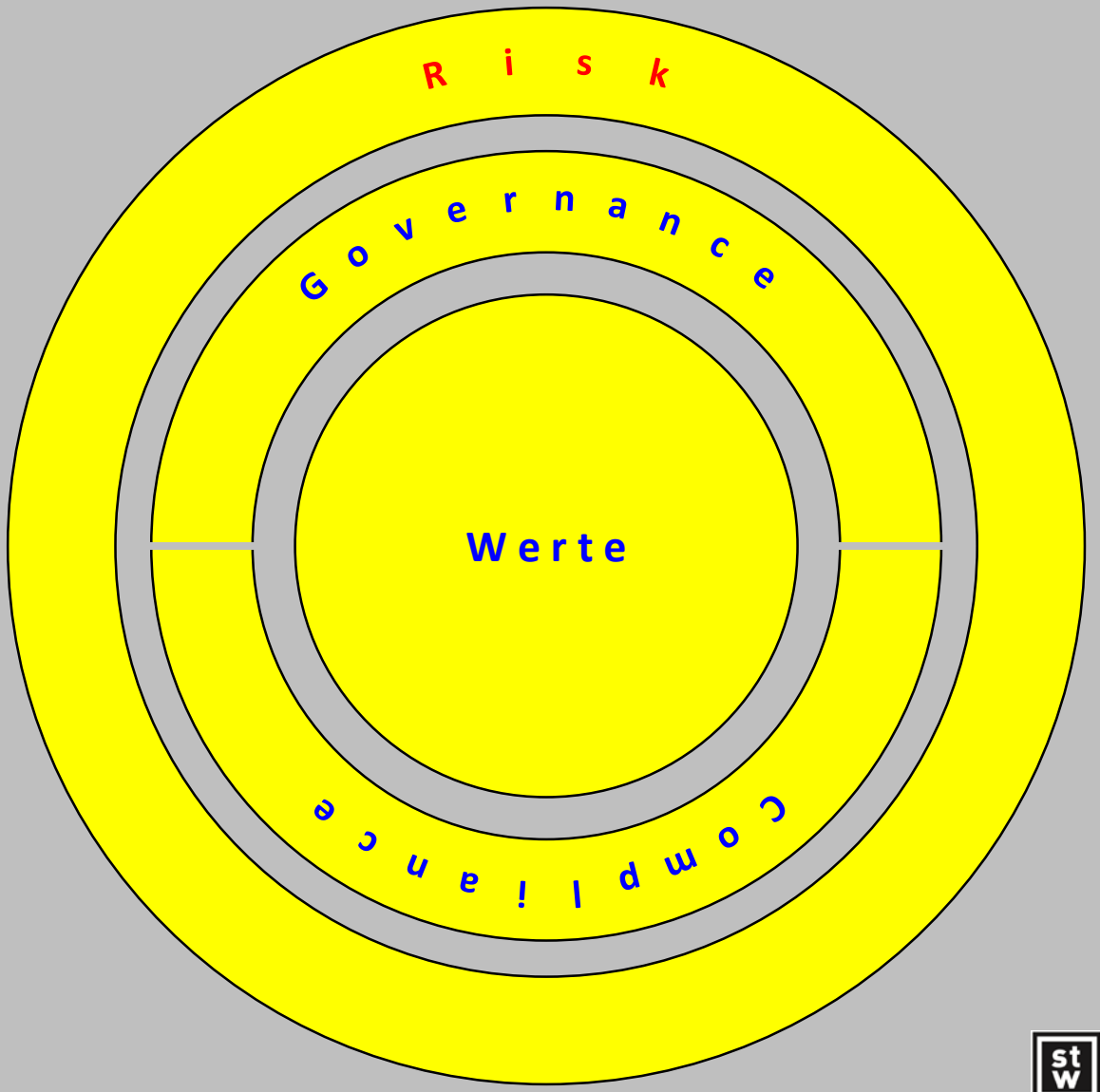
Risk / Risiko
ist die Un-Gewissheit
eines Un-Wertes.

Risiko ist ein (quantitatives)
Merkmal eines Un-Wertes.

Risikomanagement ist
Management der Un-Ge-
wissheit eines Un-Wertes.

Wertemanagement ist
Risikomanagement.

Risikomanagement ist
Wertemanagement.



Steinbeis-Transferzentrum Risikomanagement

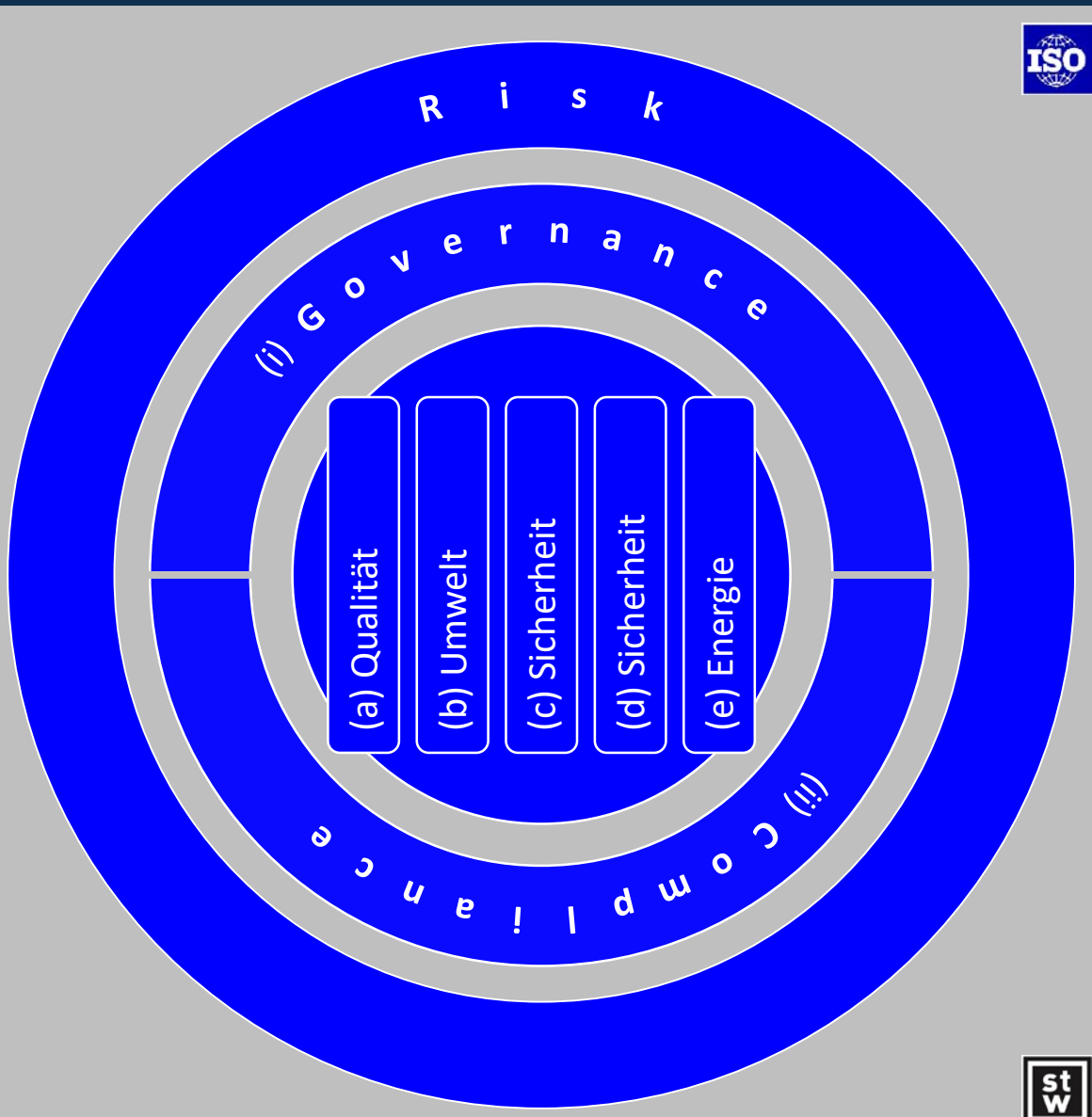
ISO XY001

Integration

von Werte- bzw. Risikomanagement für die Kategorien
(i) **Governance**§
(ii) **Compliance**§
sowie für weitere **Werte** als ISO **Werte** Themen (a) bis (e) usw.

§ zwei der ISO **Werte** Themen

(a) - (e) sind die „Silos“ für **Werte** Themen der ISO



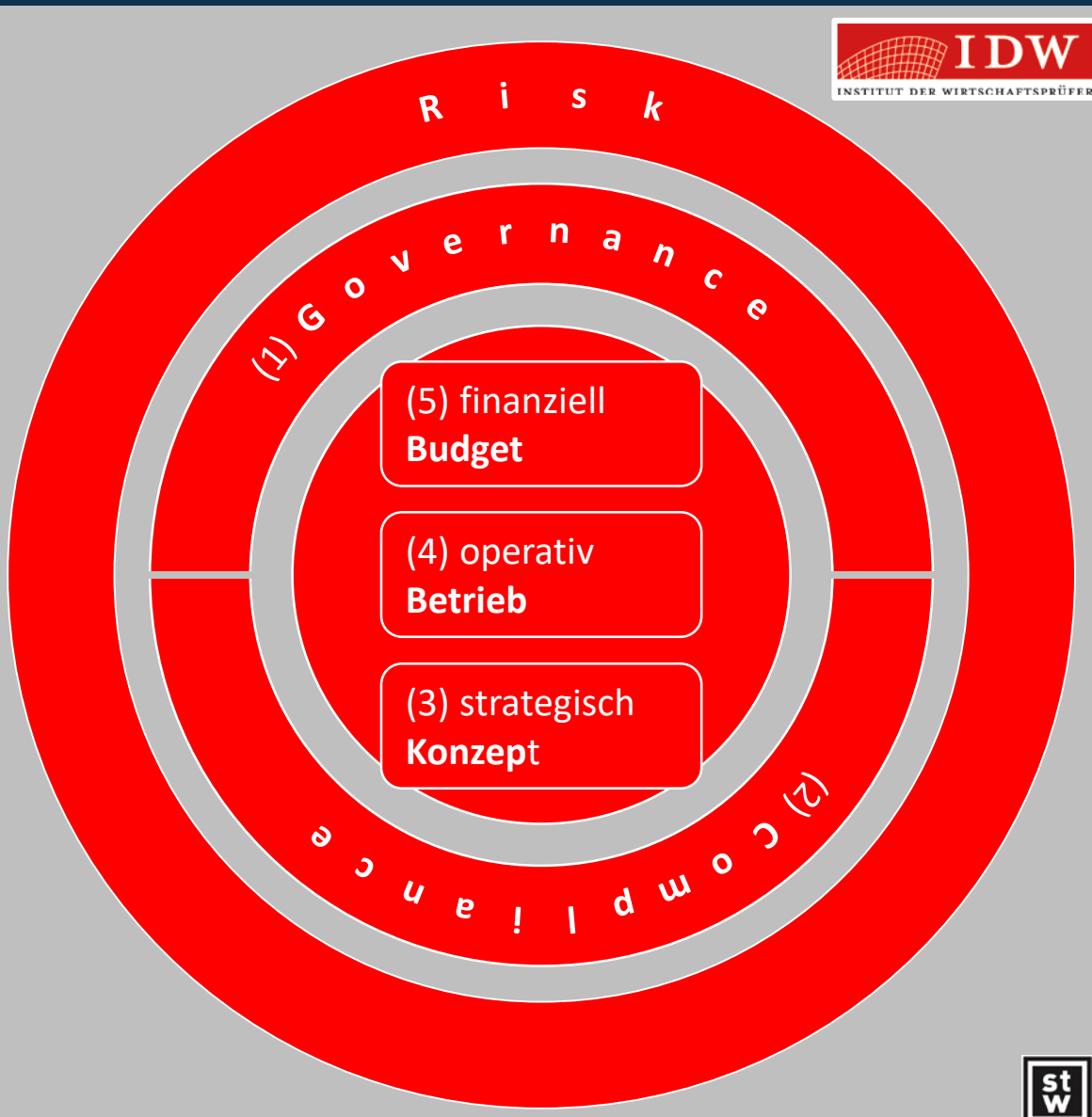
Steinbeis-Transferzentrum Risikomanagement

Integration

von Werte- bzw. Risikomanagement für die Kategorien
(1) **Governance**§
(2) **Compliance**§
sowie für weitere **Werte** als **COSO** Werte Kategorien (3) bis (5) *(erweitert)*

§ zwei COSO **Werte** Kategorien

(1) - (5) sind die „Ebenen“ für **Werte** Kategorien des COSO *(erweitert)*



Steinbeis-Transferzentrum Risikomanagement

ISO

$$Risk_{sum} = \sum_{i=1}^{i=\infty} Risk_i(ISO)$$

This set of **ISO** risk silo themes $Risk_i$ is of infinite length.

The sum of all risks is symbolically created by adding individual risks from the themes. In reality, this can be done with a numerical Monte-Carlo simulation.

i = 1: **ISO 9001** Quality
i = 2: **ISO 14001** Environment
i = 3: **ISO 27001** Safety, Security
i = 4: **ISO 45001** Safety, Security
i = 5: **ISO 50001** Energy
...
i = 1, 2, 3, …, ∞: ISO risk themes (silos)

For experts only!

COSO

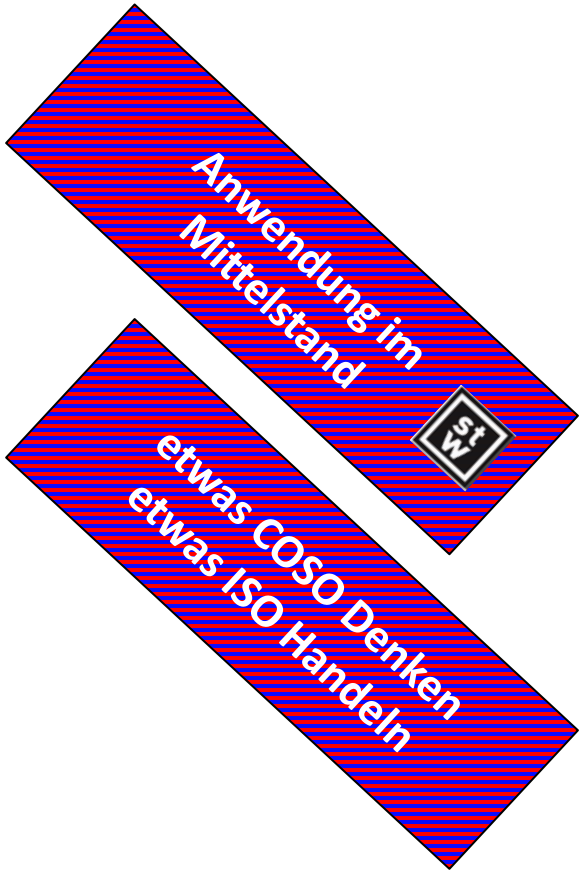
$$Risk_{total} = \sum_{j=1}^{j=5} Risk_j(COSO)$$

This set of **COSO** risk layer categories $Risk_j$ has a finite length of 5 only.

The total risk is symbolically created by adding the individual risks from the categories. In reality, this can be done with a numerical Monte-Carlo simulation.

j = 1: COSO / normative **(Governance)**
j = 2: COSO / regulative **(Compliance)**
j = 3: COSO / strategic **(Concepts)**
j = 4: COSO / operational **(Practice)**
j = 5: COSO / financial **(Report)**
...
j = 1, 2, 3, 4, 5: COSO risk categories (layers)

Meier, Peter
Sicher in die Zukunft: Umfassendes integriertes Management
Steinbeis transfer Magazin Seite 46
Heft 1; Steinbeis, Stuttgart (2018);
[ISSN 1864-1768 (Print)]



ProTec Industriebedarf GmbH

Integriertes Management

Gesetze, Regeln und (ISO) Normen zu Sachverhalten wie Qualität, Umwelt, Arbeit, Produkte, Information

Kategorien angelehnt an den Prüfungs-standard IDW PS 981 (Risikomanagement)

1. **Governance - normativ:**
   Leadership: Führung und Verantwortung
2. **Compliance - regulativ:**
   Konformität: Rechte, Regeln, Verträge
3. **Konzept - strategisch:**
   Prozesse: Qualität, Effizienz, Sicherheit
4. **Betrieb - operativ:**
   Produkte: Konformität, Sicherheit
5. **Budget - finanziell:**
   Planung: Integrität, Sicherheit, Nachhaltigkeit

10. f osi 1001:1781

Steinbeis-Transferzentrum Risikomanagement

1781 Erstveröffentlichung von Immanuel Kant's „Kritik der reinen Vernunft", KrV

Amazon ebook (2018)

KMU Leitlinien

Unternehmensweites Risikomanagement

ISO 31000:2018 für den Mittelstand

Peter Meier und Munok Kwon

Reihe Blueprint: Band 1
Steinbeis Transferzentrum Risikomanagement

Amazon ebook (2018)

Integriertes Risikomanagement

Mit dem IDW von COSO bis ISO und zurück

Peter Meier

Reihe Blueprint: Band 2
Steinbeis Transferzentrum Risikomanagement

Amazon ebook (Q2 2019)

Amazon ebook (Q2 2019)