



# Information Management LE10 – Sicherheit und Organisation

Prof. Dr. Matthias Söllner

Universitätsprofessor für Wirtschaftsinformatik und Systementwicklung  
Direktor am Wissenschaftlichen Zentrum für IT-Gestaltung (ITeG)

[soellner@uni-kassel.de](mailto:soellner@uni-kassel.de)

[www.uni-kassel.de/go/wise](http://www.uni-kassel.de/go/wise)

# Vorlesungsplan

Datum	Lerneinheit	
15.03.2024	Einführung & Grundlagen	Was will Mark Zuckerberg mit WhatsApp?
15.03.2024	Informationswirtschaft	Sind Informationen das Öl des 21sten Jahrhunderts?
18.03.2024	Informationsangebot	Ok Google...Ich bin krank. Was mache ich jetzt?
18.03.2024	Management der Daten	Wann schlägt Mensch Maschine?
19.04.2024	Management der Prozesse	Was geht in meinem Unternehmen eigentlich so vor?
19.04.2024	Management von Anwendungen	Warum für Software bezahlen, wenn es Open Source gibt?
22.04.2024	Innovative IKT	Warum gibt mein Chef mir nicht endlich ein Macbook Air?
22.04.2024	Wartung und Betrieb der IKT	Kann ein ehemaliges Staatsunternehmen überhaupt Innovativ sein?
03.05.2024	Speicherung und Kommunikation	Wird der FC Luzern doch der nächste Meister?
03.05.2024	Sicherheit und Organisation	Woher weiß ich, dass hier jeder nur das sieht, was er sehen soll?
06.05.2024	Führungsaufgaben	Wie kann ich alle IT-Themen unter einen Hut kriegen?
06.05.2024	Klausurvorbereitung	Was möchte ich nochmal erklärt haben?

## Lernziele LE10



- 1) Sie sind vertraut mit dem Management und kennen wichtige **Standards** und **Rahmenwerke** zur **Informationssicherheit**.
- 2) Sie verstehen das **Ebenenmodell** der **Sicherung von Informationen** und kennen die **Risikomanagementprozesse** im Informationsmanagement.
- 3) Ihnen ist **IT-Grundschutz-Rahmenwerk** geläufig.

# Sony Pictures Entertainment



- Im November 2014 wurde Sony Pictures Entertainment Opfer eines Hackerangriffs
- Es wurde eine große Menge interner Daten und unveröffentlichte Filme entwendet
- Die Hacker drohten damit das Material zu veröffentlichen, wenn der Nordkorea-Satire-Film „The Interview“ nicht zurückgezogen wird
- Die US-Regierung beschuldigt die nordkoreanische Regierung für den Angriff verantwortlich zu sein
- Der Angriff war die größte Cyberattacke, die sich bislang gegen ein privates Unternehmen in den USA gerichtet hat
- Der entstandene Schaden wird auf bis zu 100 Mio. US-\$ geschätzt

Quelle: <http://www.spiegel.de/politik/ausland/sony-hack-obama-kuendigt-konsequenzen-fuer-nordkorea-an-a-1009699.html>, <http://www.manager-magazin.de/unternehmen/it/sony-filmstudio-hackerschaden-ist-von-versicherung-gedeckt-a-1012169.html>

# 12 Massnahmen zur Absicherung gegen Angriffe aus dem Internet des BSI



## Kernmassnahmen

- 1) Sicherheitsupdates regelmäßig installieren
- 2) Aktuelles Virenschutzprogramm verwenden
- 3) Personal Firewall verwenden
- 4) Internet nur mit Benutzerkonto mit eingeschränkten Rechten nutzen
- 5) Seien Sie zurückhaltend mit der Weitergabe persönlicher Informationen. Seien Sie misstrauisch (Link bzw. E-Mail Anhang)

## Ergänzende Massnahmen

- 6) Modernen Browser mit Filtermechanismen verwenden
- 7) Möglichst sichere Passwörter verwenden
- 8) Persönliche Daten nur über verschlüsselte Verbindungen übertragen
- 9) Nicht benötigte Programme deinstallieren
- 10) Regelmäßig Sicherheitskopien erstellen
- 11) WLAN mit WPA2 verschlüsseln bzw. nur solches verwenden
- 12) Regelmäßig den Sicherheitsstatus des Computers überprüfen

## Zusammenarbeit BSI und ISB

- In D ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) für den IT-Grundschutz verantwortlich
- In der Schweiz ist es das Informatiksteuerungsorgan des Bundes (ISB) mit Sitz in Bern
- Es besteht eine internationale Kooperation der D und CH Behörden, sowie den Behörden aus Österreich (Zentrum für sichere Informationstechnologie Austria, A-SIT) und Luxembourg (Cyberworld awareness & security enhancement, Cases)

# Agenda LE10 – Sicherheit und Organisation

1

Management der Informationssicherheit

2

Ebenen der Sicherung von Informationen

3

Risikomanagement

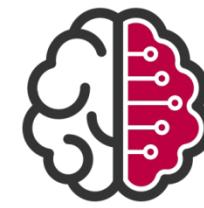
4

Managementsysteme

5

IT-Grundschutz

# 1. Management der Informationssicherheit



W I S E

## Begriffserklärung (I)

**Sicherheit** ist die Freiheit von unvertretbaren Risiken (DIN 2002)

Das Wort “**Sicherheit**” besitzt im Englischen zwei Äquivalente:

**Safety:** Schutz vor **unbeabsichtigte Ereignisse**, wie Feuer- bzw. Wasserschäden, Naturkatastrophen oder Verarbeitungsfehler.

**Security:** Schutz vor **beabsichtigte Angriffe**, wie Computer-Viren, Abhören oder Datendiebstahl.

## Begriffserklärung (II)

Das Ziel der **Informationssicherheit**, das heisst, der Sicherheit im Rahmen des Informationsmanagements, ist der angemessene **Schutz aller Informationen** im Unternehmen. Dies umfasst sowohl **elektronisch gespeicherte Daten** als auch Daten auf **traditionellen Medien**, wie etwa Papier und Expertenwissen, das in den **Köpfen der Mitarbeiter** internalisiert wurde (Krcmar 2015).

**IT-Sicherheit** ist die Reduzierung der Informationssicherheit auf den Schutz der **elektronisch gespeicherten Informationen** und deren **Verarbeitung**. IT-Sicherheit ist dementsprechend eine **Untermenge der Informationssicherheit**.

## Begriffserklärung (III)

Ein **Risiko** ist eine mögliche Zielabweichung auf Grund zukünftiger Systemzustände unter Berücksichtigung möglicher Handlungsoptionen (Adams 1995, Schermann 2011).

- Wesentliche Bestandteile des Risikobegriffs (Schermann 2011, Wolf 2005):
  - Zur Betrachtung zukünftiger Systemzustände ist es notwendig, die **Ursache** zu kennen
  - Gleichzeitig muss die **Wirkung** des betrachteten Systemzustands auf die verfolgten Ziele analysiert werden
  - Anschliessend erfolgt eine kontinuierliche **Bewertung** dieser beiden Aspekte von Ursache und Wirkung

## Begriffserklärung (IV)

- Die klassischen **Grundwerte der Informationssicherheit** nach (BSI 2006) :

**Vertraulichkeit:** Informationen sollen nur für einen bestimmten Personenkreis **zugänglich** sein; die **Weitergabe** an Dritte oder der Zugriff unbefugter Personen muss entsprechend **verhindert** werden.

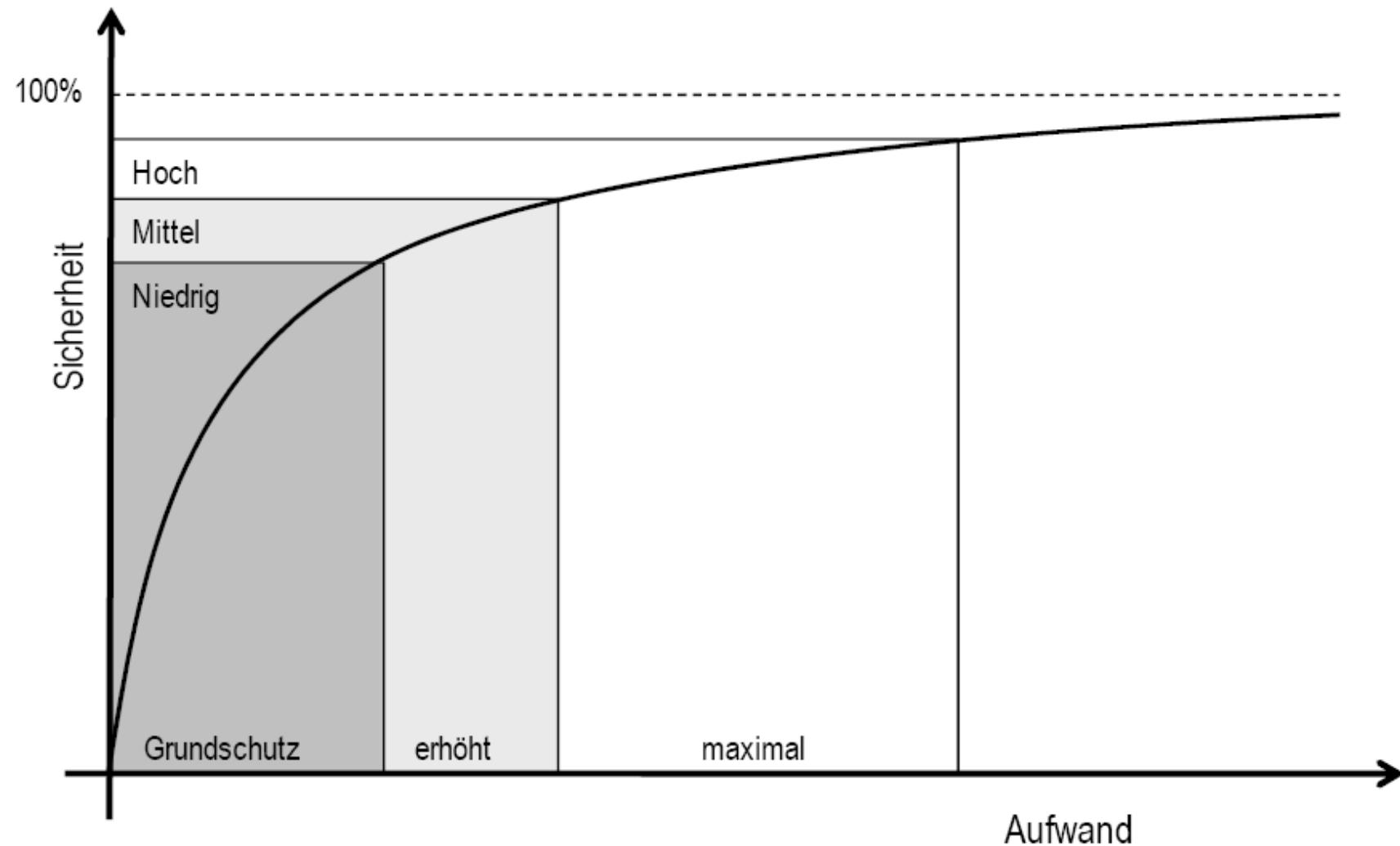
**Integrität:** Die **Vollständigkeit, Unverfälschtheit und Konsistenz** von Informationen muss gewährleistet werden. **Veränderung** von Informationen können **bewusst, unabsichtlich** oder durch **Verarbeitungsfehler** verursacht werden.

**Verfügbarkeit:** Informationen müssen zum **richtigen Zeitpunkt** und in der **richtigen Menge** zur Verfügung gestellt werden. Die **Performanz** und die **Erreichbarkeit** sind ebenso entscheidend wie Ausfallsicherheit

## Aufwand-Nutzen-Relation für Informationssicherheit

- Es können Korrelationen zwischen den Eintrittswahrscheinlichkeiten der Gefahren auftreten.
  - Stromausfall bei Erdbeben wahrscheinlicher als im Normalfall
  - Bildung von Risikoportfolien
- Als sicher gilt ein Zustand dann, wenn die Eintrittswahrscheinlichkeit von Risiken oder Gefahrenpotential gleich Null sind.
  - Gefahr eines Erdbebens der Stärke VI-VII in Garching wurde mit  $10^{-5}$  / Jahr beziffert

# Aufwand-Nutzen-Relation für Informationssicherheit



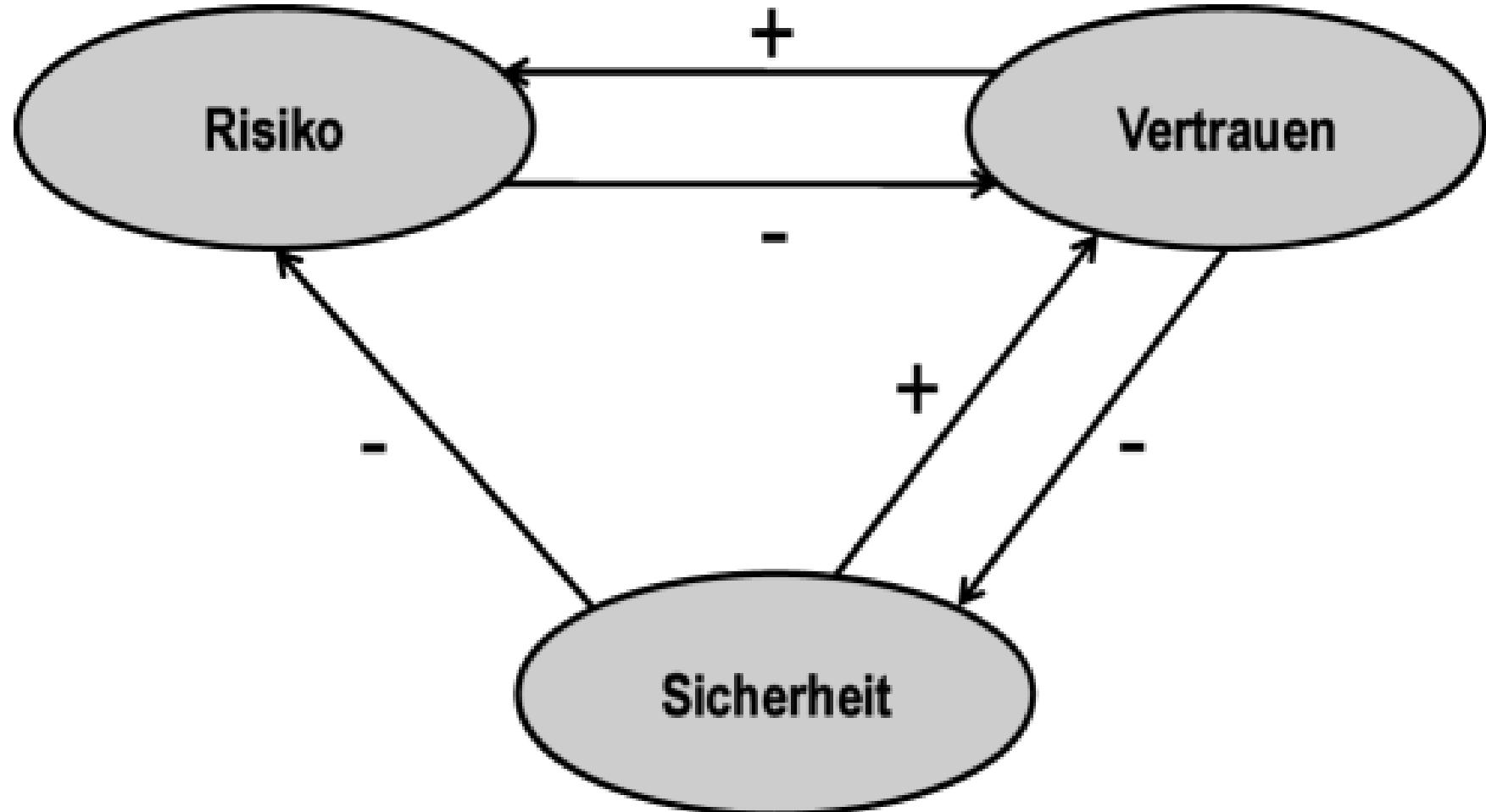
## Vertrauen zur Komplexitätsreduktion

Um die Massnahmen des Managements der Informationssicherheit in einem Dreiklang zwischen Vertrauen, Sicherheit und Risiko definieren zu können, muss der Begriff Vertrauen erläutert werden.

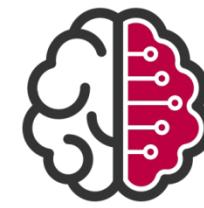
“Vertrauen ist die **freiwillige Erbringung** einer **riskanten Vorleistung** unter Verzicht auf explizite vertragliche **Sicherungs- und Kontrollmassnahmen** [...] in der **Erwartung**, dass der **Vertrauensnehmer** motiviert ist, freiwillig auf **opportunistisches Verhalten** zu verzichten” (Ripperger 1998).

**Vertrauen** reduziert die Komplexität der Umwelt auf ein handhabbares Mass und stellt eine Vorleistung dar, die Interaktion erst ermöglicht (Luhmann 2000).

# Dreiklang aus Risiko, Vertrauen und Sicherheit



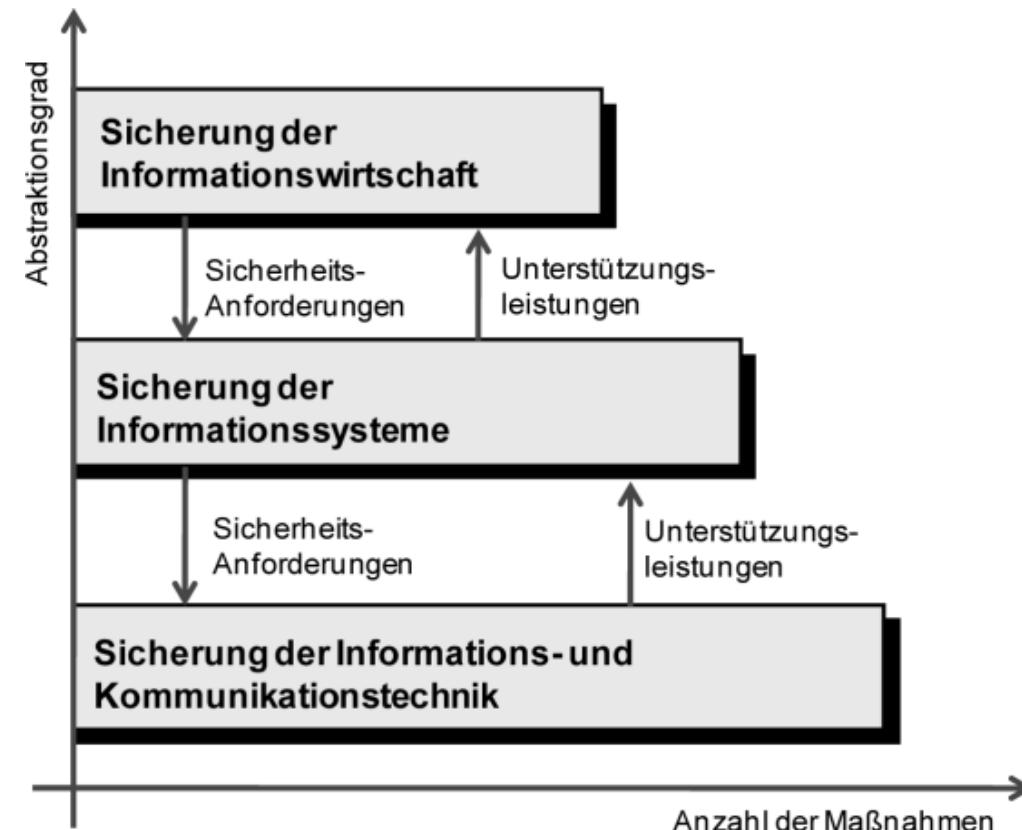
## 2. Ebenen der Sicherung von Informationen



W I S E

# Ebenen der Sicherung von Informationen

- Das Management der Informationssicherheit kann in drei Ebenen gegliedert werden. Oberstes Ziel ist die Sicherung der Informationswirtschaft.



# Ebenen der Sicherung von Informationen

## Sicherung der Informationswirtschaft:

- Auf der Managementebene wird das Gleichgewicht durch organisierte Massnahmen vor Risiken geschützt und präventiv gesichert.
- Das Gleichgewicht bezieht sich auf Angebot, Nachfrage, Qualität und Informationsfluss
- Sicherheitsrelevante Objekte der Informationswirtschaft werden definiert um daraus Anforderungen, Sicherheitsziele und -leitlinien abzuleiten
  - Eine Richtlinie im Krankenhaus, dass Informationen über die Patienten nur im Krankenhaus bearbeitet werden dürfen.

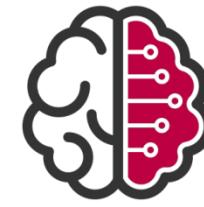
## Sicherung des Informationssystems:

- Umsetzung der Informationslogistik durch IT-Sicherheitskonzept.
- Die Anforderungen der Informationswirtschaft werden in technische Anforderungen für die Informationssysteme übersetzt.
  - Verteiltes IS, das Zertifikate für die Identifikation verwendet, um die Anforderung der Authentifizierung umzusetzen.

## Sicherung der IKT (IT-Sicherheit):

- Schutz von Prozessen (Speicherung, Verarbeitung und Kommunikation) mit Verfügung stehenden Ressourcen.
  - Redundante Datenhaltung, Verschlüsselung

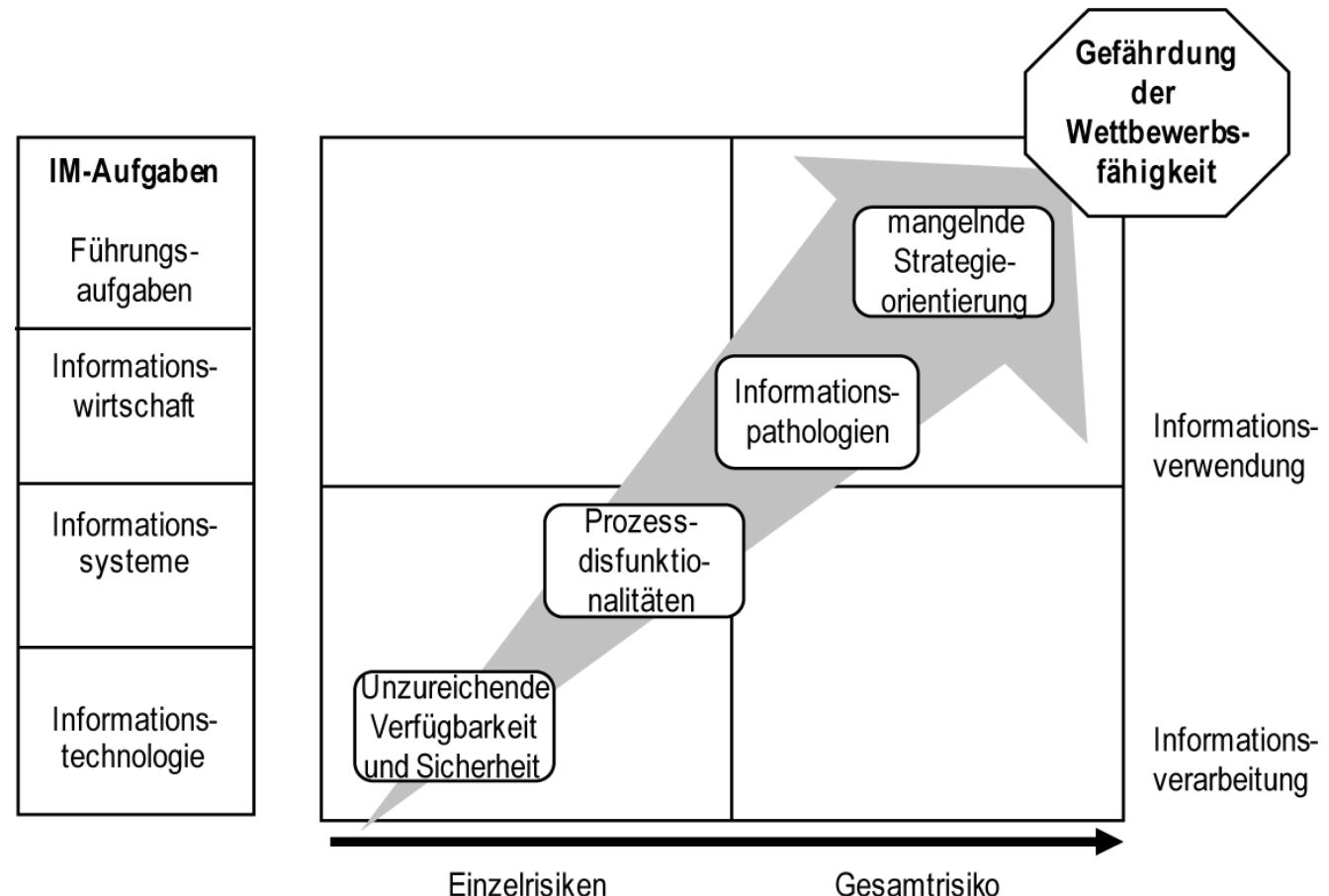
### 3. Risikomanagement



W I S E

# Risiken des Informationsmanagements

- Im Ebenenmodell des IM kann jeder Ebene eine spezifische Risikokategorie zugeordnet werden



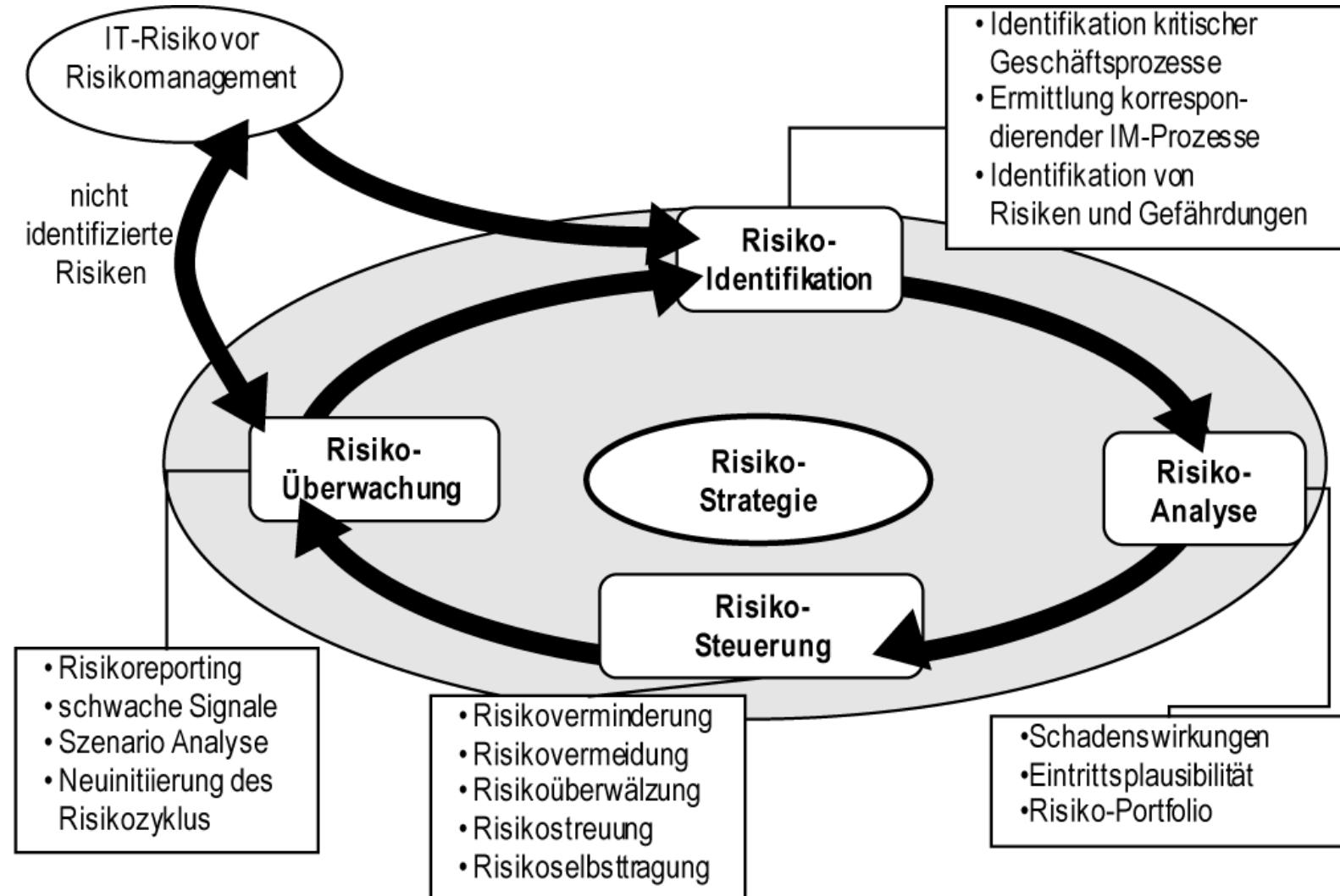
# Beispiele für Risiko

Subjekt	Zielabweichung	Systemzustände	Alternativen
Kernkraft	GAU, Angst, Austritt von Radioaktivität	Erdbeben, Stromausfall, Tsunami	abschalten, schützen, verlagern
Flugverkehr	Absturz, Verspätung, Flugausfall	Technische Fehler, Gewitter, Entführung	Bahnfahren, Autofahren, nicht reisen
Dezentrale Datenspeicherung	Verlust, keine Verfügbarkeit	Ausfall der Festplatte, Diebstahl der HW, Virus	Daten sichern, zentral speichern
Zentrale Datenspeicherung	Keine Verfügbarkeit, Verlust, Datendiebstahl, Inkompatibilität	Hacker Angriff (DoS), Stromausfall, Erdbeben	Verschlüsseln, spiegeln, dezentral speichern

# Social Media Risiken



# Risikomanagementprozess im Informationsmanagement



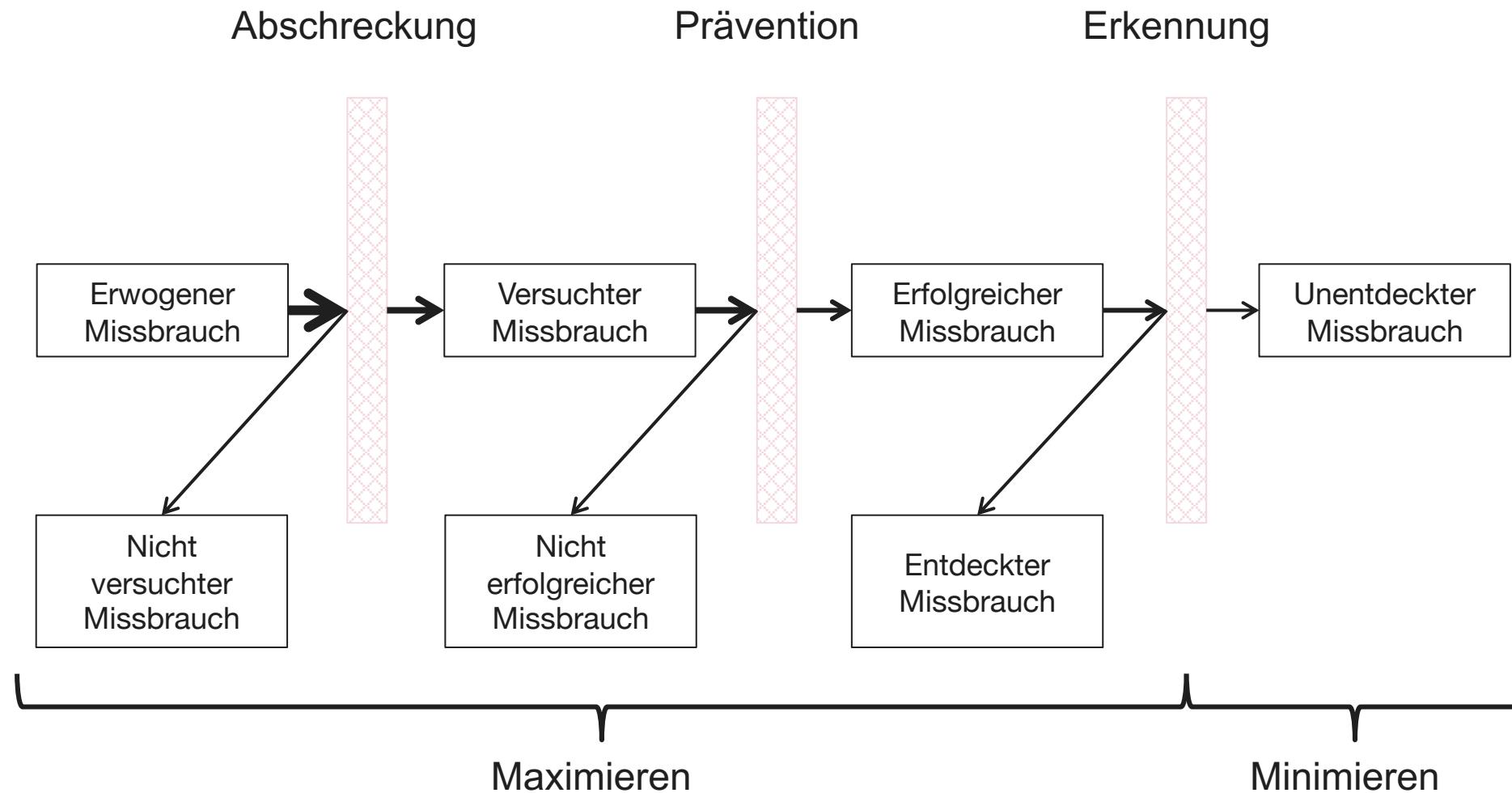
# Risikosteuerung

- Für die Umsetzung einer **effektiven** und **effizienten** Risikosteuerung in Bezug auf die Informationssicherheit bedarf es
  - detaillierter **Kenntnisse** über die Ursachen und Wirkungen von Risiken der Informationssicherheit
  - eines **Prozesses** für die systematische Durchführung der Aktivitäten des Risikomanagements sowie
  - einer **organisatorischen Umsetzung** des Risikomanagements.

# Strategien zur Risikosteuerung

Steuerungsstrategie	Massnahmen	Anwendungsbereiche	Beispiele
<b>Risikovermeidung</b>	Extremfall der Risikoverminderung auf ein Restrisiko von null	Vorwiegend bei Risikoeinstufung „sehr hoch“ oder „hoch“	Abschaffung eines Systems, Abbruch des Projekts
<b>Risikoverminderung</b>	Reduktion der Eintrittsplausibilität und Verringerung der Schadenswirkungen, aktive Beeinflussung der Ursachen sowie antizipatives Handeln des IM	Vorwiegend bei Risikoeinstufung „hoch“ oder „mittel“	Einführung von redundanten Systemen, Backup von Daten
<b>Risikoüberwälzung</b>	Übertragung möglicher Störungen vor ihrem Eintritt auf andere Wirtschaftssubjekte	Anwendung bei allen Risikoeinstufungen möglich. Beschränkung meist auf reine Risiken (bspw. Betriebsrisiken im Rechenzentrum)	Abschluss einer Versicherung , Outsourcing,
<b>Risikoselbsttragung</b>	Bewusste Akzeptanz des (Rest-) Risikos, im Rahmen unternehmerischen Handelns nicht eliminierbar	Management des akzeptierten Restrisikoniveaus („niedrig“, „vernachlässigbar“) nach erfolgter Risikosteuerung	Versand unverschlüsselter E-Mails, Bildung von finanziellen oder materiellen Reserven
<b>Risikostreuung</b>	Zerlegung eines Gesamtrisikos in beherrschbare Einzelrisiken	Komplexe Prozess- oder Geschäftsmodellrisiken	Globale Verteilung wichtiger Anwendungssysteme

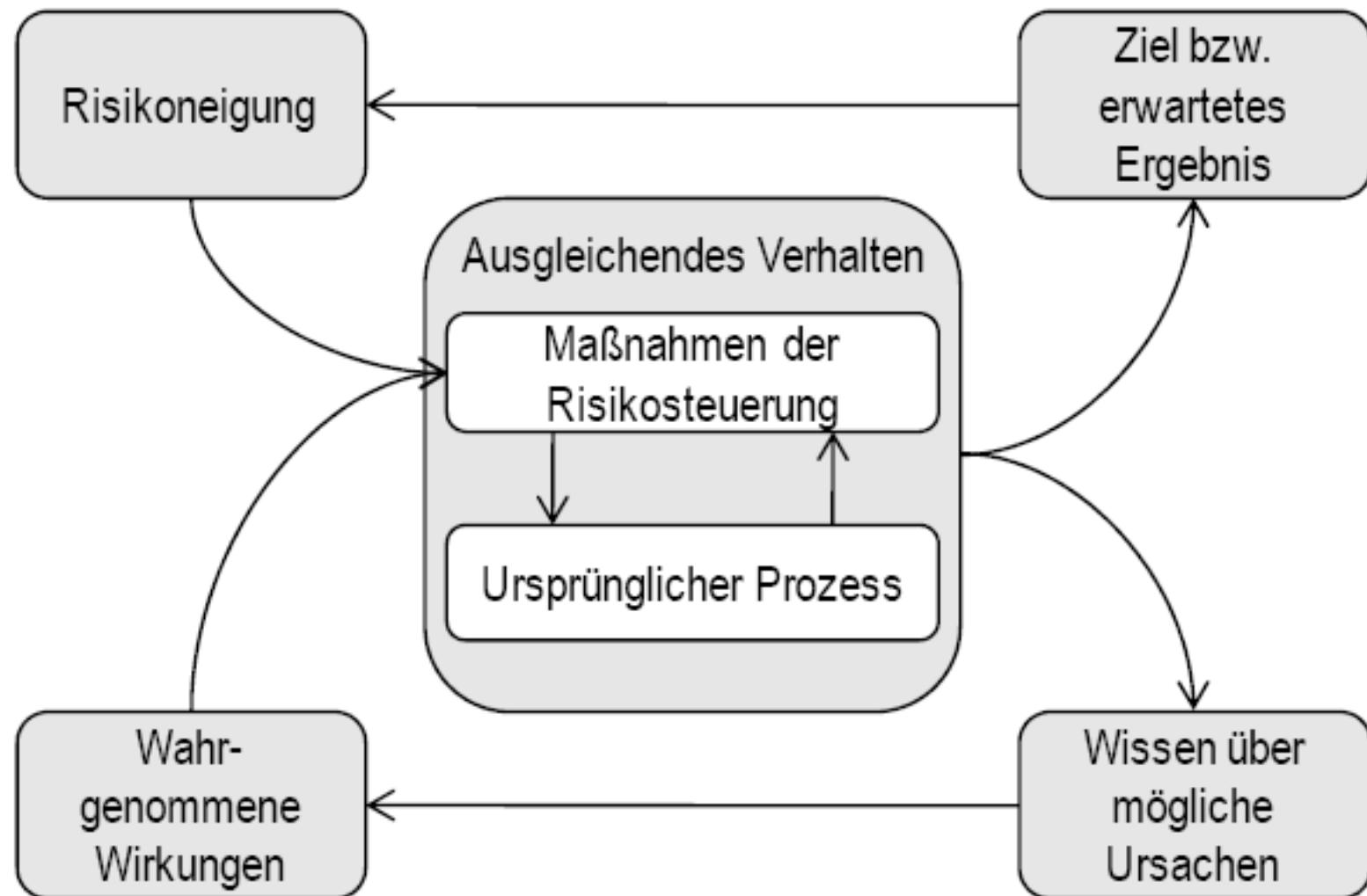
# Risikosteuerung durch Abschreckung, Prävention und Erkennung



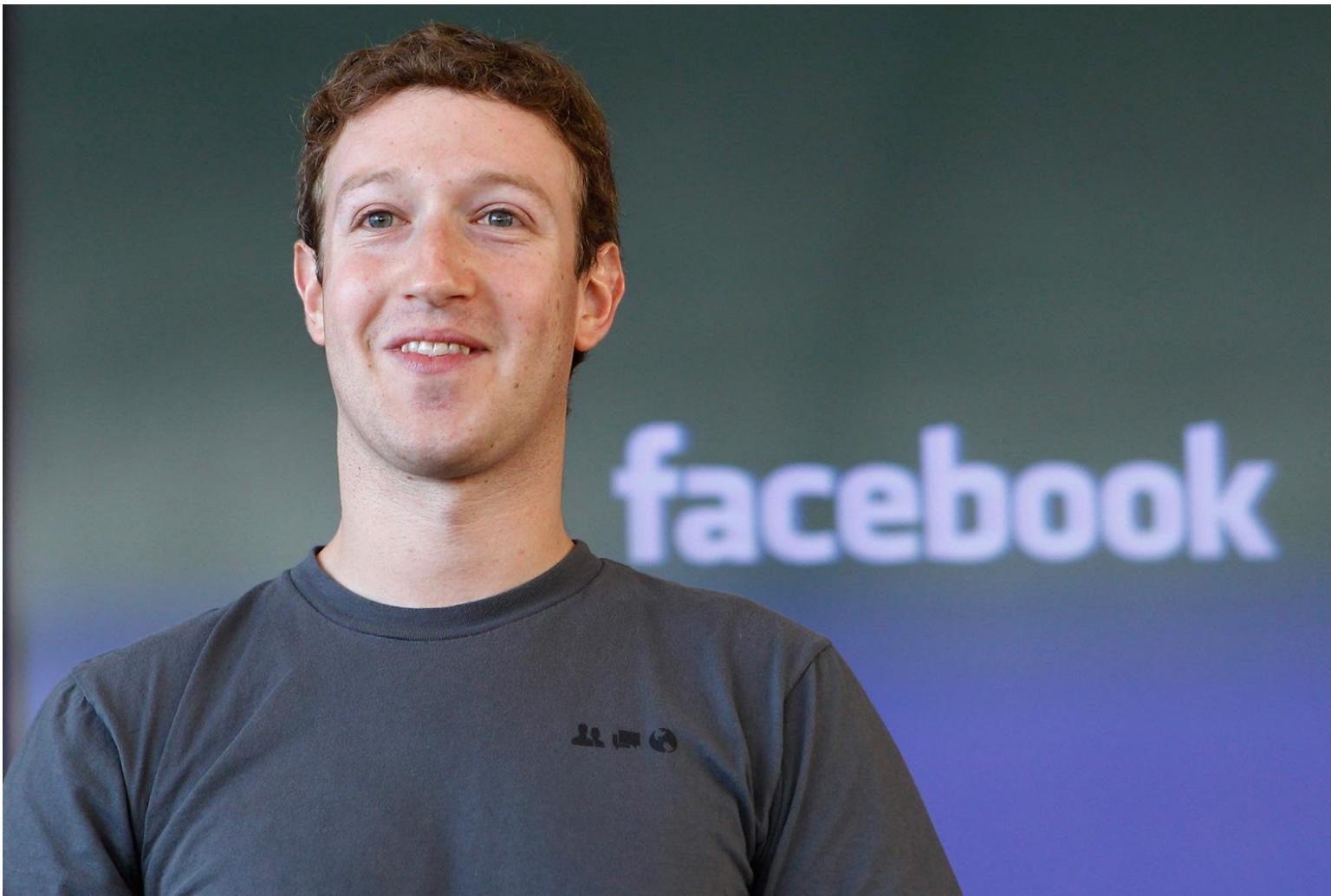
## Ursachen und Wirkung von Risiken

- Für eine effektive Steuerung von Risiken sind Informationen zur Ursachen und Wirkungen von Risiken notwendig, um Massnahmen zur Verminderung oder Vermeidung von Risiken zu entwickeln und bewerten.
- Kenntnisse über die Wirkung von Massnahmen erlauben:
  - Beurteilung der Relevanz eines bestimmten Risikos
  - Untersuchung zur Reduzierung der Risikowirkung
  - Wirkung von möglichen Steuerungsmassnahmen

# Ursachen und Wirkungen von Risiken

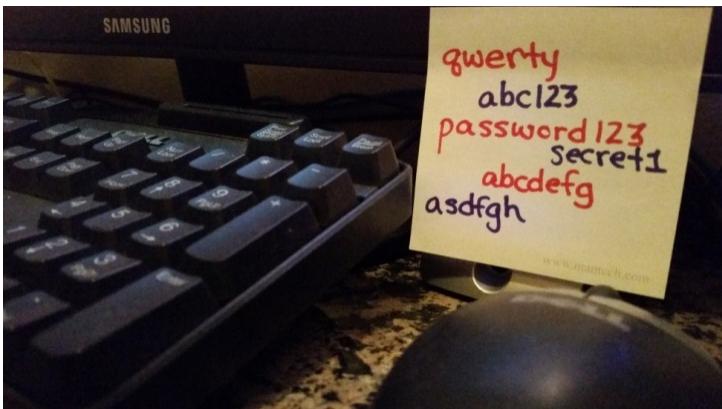


Was könnte dieser Mann mit schlechten Passwörtern zu tun haben?



# Mitarbeiter und Risikomanagement

- Mitarbeiter stellen das schwächste Glied dar:
  - Über die Hälfte der Sicherheitsbrüche werden indirekt oder direkt durch mangelnde Einhaltung von IT Sicherheitsregeln verursacht (Dhillon and Moores 2001; Stanton et al. 2005)
  - Beispiele:
    - Unvorsichtiges Öffnen von E-Mail Anhängen
    - Triviale Passwörter
    - Ein Passwort für alle Systeme
    - Update der Rechner wird nur unregelmässig durchgeführt



# Top 10 Schweizer Passwörter (2017)

- 1.** 123456
- 2.** 1234
- 3.** 123456789
- 4.** 12345678
- 5.** 12345
- 6.** 11.11.11
- 7.** hallo
- 8.** passwort
- 9.** soleil
- 10.** password

# Mitarbeiter und Risikomanagement

- Möglichkeit Mitarbeiter zur Einhaltung von Sicherheitsregeln zu bewegen:

## Kampagnen

Mitarbeiter werden über die Folgen von Verletzungen von Sicherheitsregeln informiert

## Sanktionen

Mitarbeiter wissen, dass sie für die Verletzung von Sicherheitsregeln bestraft werden können

## Partizipation

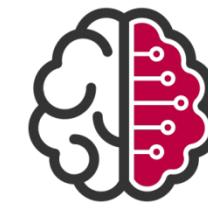
Mitarbeiter werden bei der Entwicklung von Sicherheitsregeln und -systemen miteinbezogen.

# Mitarbeiter und Risikomanagement

- Beispiel für eine Poster Kampagne

CHECK OUT THE TOP 20 <b>WORST PASSWORDS</b> ARE ANY OF YOURS IN THIS LIST?	
1 123456	2 password
3 12345678	4 qwerty
5 abc123	6 123456789
7 111111	8 1234567
9 iloveyou	10 adobe123
11 123123	12 admin
13 1234567890	14 letmein
15 photoshop	16 1234
17 monkey	18 shadow
19 sunshine	20 12345

# 4. Managementsysteme



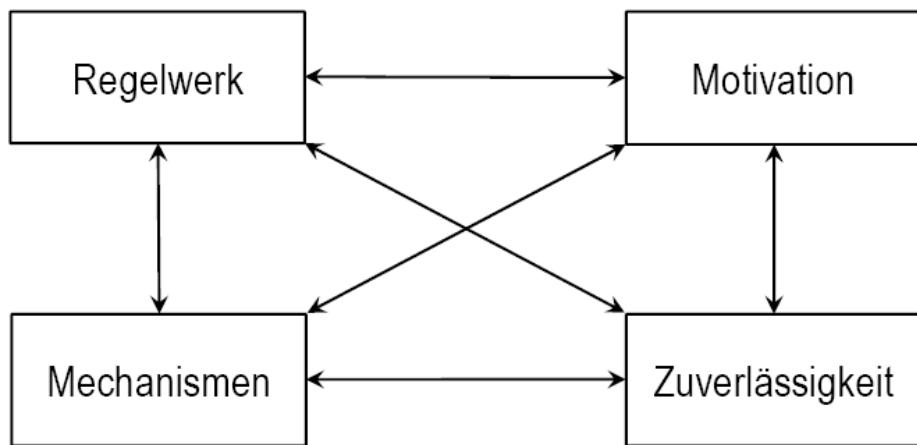
W I S E

# Managementsysteme für Informationssicherheit

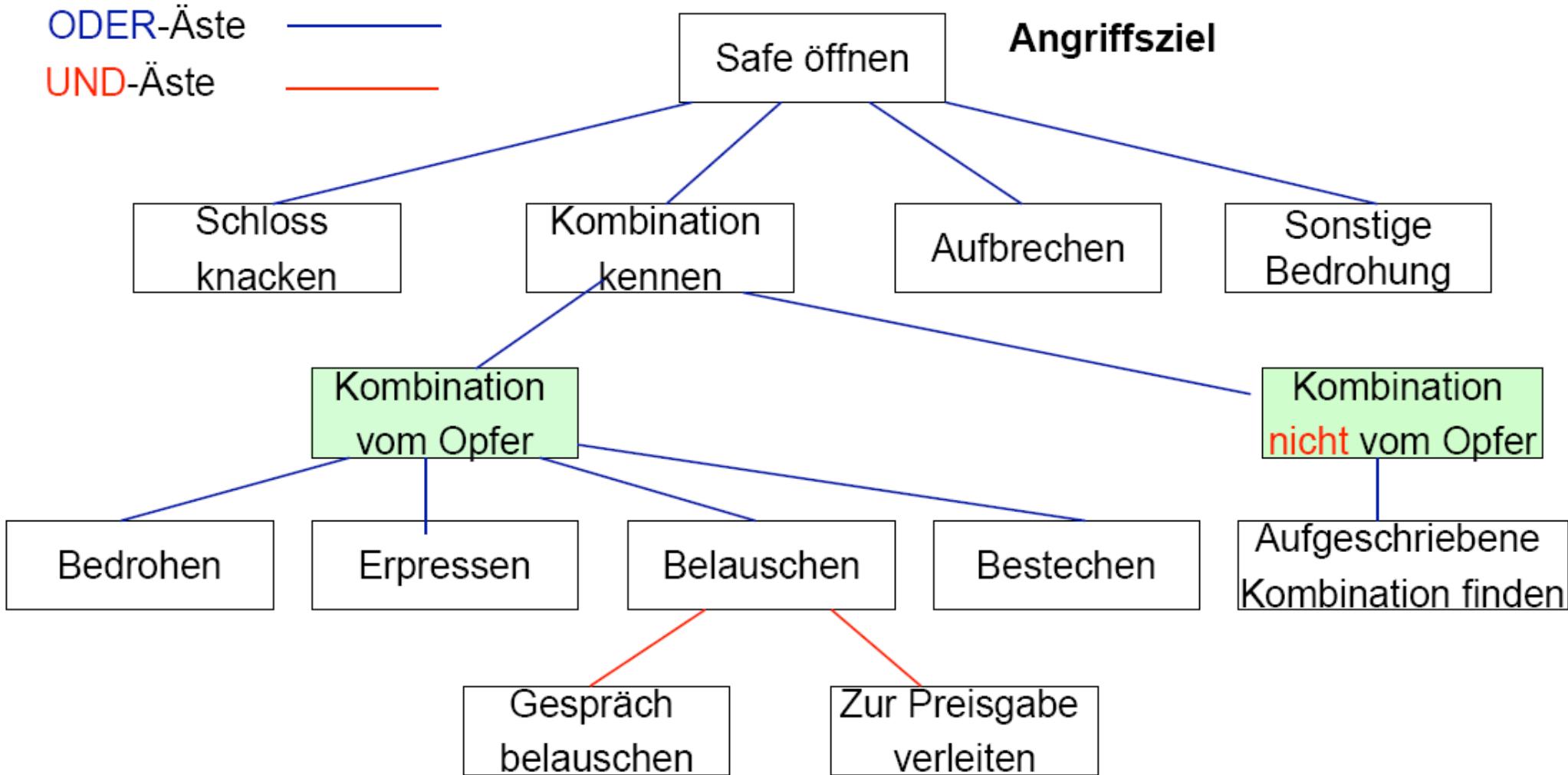
- Sicherheitsmanagement ist ein **kontinuierlicher Prozess**, der die Sicherheit und die Zuverlässigkeit von IS innerhalb einer Organisation gestaltet.
- **Kernaufgaben:**
  - Festlegung von Sicherheitsstrategie, -zielen, und –politik der Organisation,
  - Festlegung der Sicherheitsanforderungen,
  - Festlegung und Bewertung geeigneter Gegenmassnahmen (u. a. auch Grundschutzmassnahmen),
  - Überwachung der Implementierung und des laufenden Betriebes der ausgewählten Massnahmen,
  - Förderung des Sicherheitsbewusstseins innerhalb der Organisation
  - Entdeckung von Reaktionen auf sicherheitsrelevante Ereignisse.

# Rahmenbedingungen für das Sicherheitsmanagement

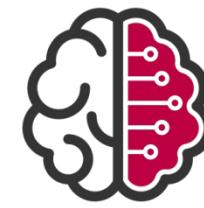
- das **Regelwerk**, das die umzusetzenden Sicherheitsrichtlinien identifiziert, analysiert und festlegt;
- die **Mechanismen**, durch die das Regelwerk umgesetzt wird;
- die **Zuverlässigkeit** der einzelnen Mechanismen;
- die **Motivation** der Nutzer des Systems (Schutz und Aufrechterhaltung des sicheren Betriebes) als auch die Beweggründe potentieller Angreifer.



# Angriffsbaum



# 5. IT-Grundschutz



W I S E

# IT-Grundschutz

- Das **Ziel** des Grundschatzansatzes ist es, eine **minimale Menge** von **Sicherheitsmassnahmen** zu errichten, um alle oder einige **IT-Systeme** einer Organisation zu **schützen**.
- Einteilung:
  - **BSI-Standards**: Diese enthalten Empfehlungen des BSI zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Massnahmen mit Bezug zur Informationssicherheit.
  - **IT-Grundschutz-Kataloge**: Es schlägt Sicherheitsmassnahmen gegen Bedrohungen vor, um ein IT-System zu schützen. Es besteht aus Bausteinen, die jeweils Gefährdungen und geeignete Massnahmen dagegen enthalten.
- Die Dokumente zum IT-Grundschatz werden vom **Bundesamt für Sicherheit in der Informationstechnik (BSI)** erstellt.

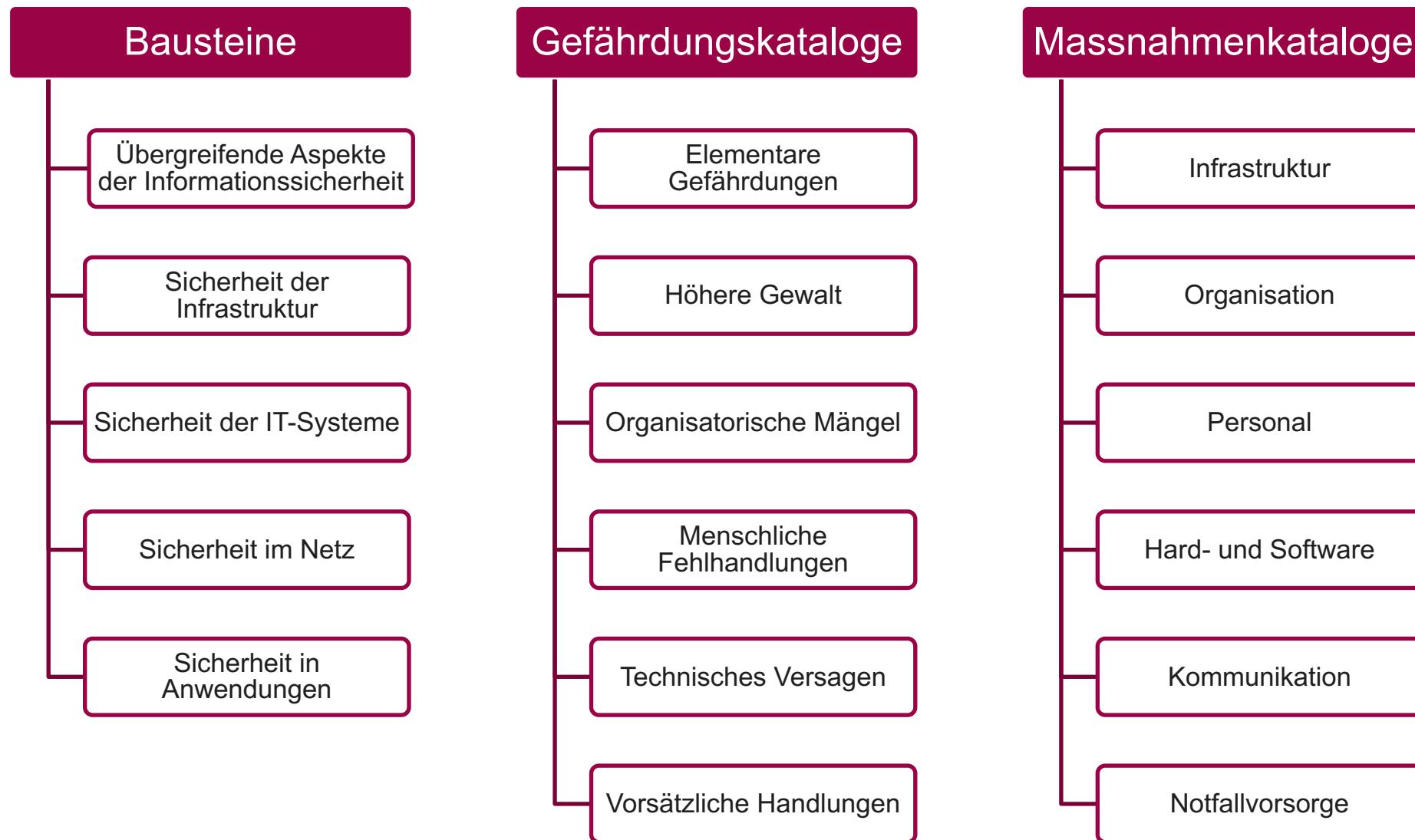
## BSI Standards (1/2)

- BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS):
  - definiert allgemeine Anforderungen an ein ISMS
  - Beispiel – Einbindung der Mitarbeiter in den Sicherheitsprozess: „Werden Mitarbeiter neu eingestellt oder erhalten neue Aufgaben, ist eine gründliche Einarbeitung und Ausbildung notwendig. Die Vermittlung sicherheitsrelevanter Aspekte des jeweiligen Arbeitsplatzes muss dabei berücksichtigt werden.“
- BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
  - beschreibt Schritt für Schritt, wie ein Managementsystem für Informationssicherheit in der Praxis aufgebaut und betrieben werden kann
  - Beispiel – Auswahl und Anpassung von Massnahmen: „Nachdem die notwendigen Informationen aus der Strukturanalyse und der Schutzbedarfsfeststellung vorliegen, besteht die nächste zentrale Aufgabe darin, den betrachteten Informationsverbund mit Hilfe der vorhandenen Bausteine aus den IT-Grundschutz-Katalogen nachzubilden. Als Ergebnis wird ein IT-Grundschutz-Modell des Informationsverbunds erstellt“

## BSI Standards (2/2)

- BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
  - erläutert eine Vorgehensweise um Zielobjekte, die einen hohen Schutzbedarf haben oder in den IT-Grundschutz-Katalogen noch nicht behandelt werden, zu schützen.
  - Beispiel – Risiken unter Beobachtung: „Bei der Risikoanalyse können unter Umständen Gefährdungen identifiziert werden, aus denen Risiken resultieren, die zwar derzeit akzeptabel sind, in Zukunft jedoch voraussichtlich steigen werden. Dies bedeutet, dass sich in der weiteren Entwicklung ein Handlungsbedarf ergeben könnte.“
- BSI-Standard 100-4: Notfallmanagement
  - zeigt einen systematischen Weg auf, ein Notfallmanagement in einer Behörde oder einem Unternehmen aufzubauen, um die Kontinuität des Geschäftsbetriebs sicherzustellen
  - Beispiel – Notfallvorsorgekonzept: „Das Notfallvorsorgekonzept bildet die Grundlage zur Umsetzung der Kontinuitätsstrategien. Es beschreibt die vorliegenden Bedingungen und beinhaltet alle bei der Konzeption anfallenden Informationen.“

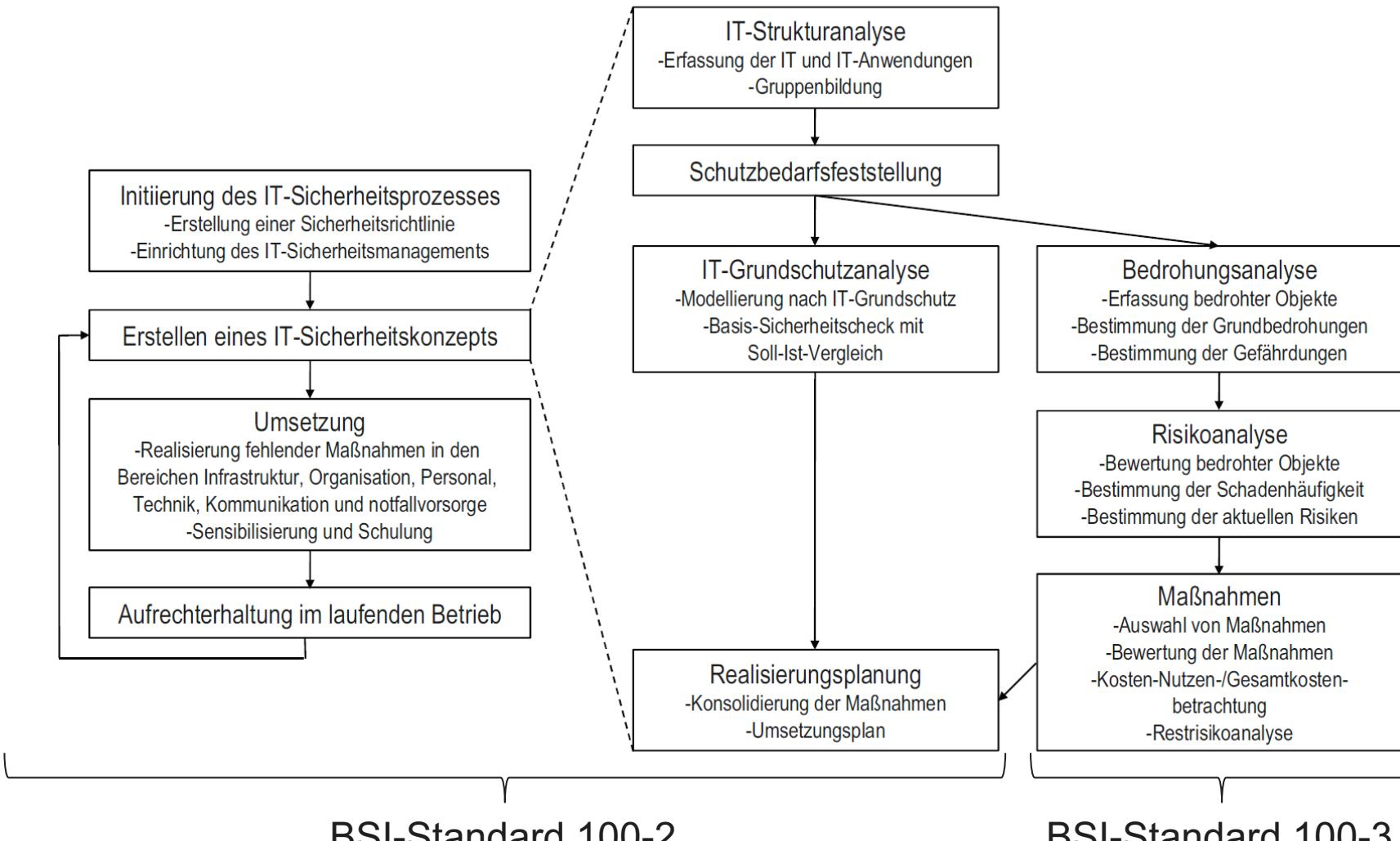
# Aufbau der IT-Grundschutz-Kataloge



# Beispiel - B 2.2 Elektrotechnische Verkabelung

Gefährdungslage	Massnahmenempfehlung
<p><b>Höhere Gewalt</b></p> <ul style="list-style-type: none"><li>- G 1.6 Kabelbrand</li></ul> <p><b>Organisatorische Mängel</b></p> <ul style="list-style-type: none"><li>- G 2.11 Unzureichende Trassendimensionierung</li><li>- G 2.12 Unzureichende Dokumentation der Verkabelung</li><li>- G 2.13 Unzureichend geschützte Verteiler</li></ul> <p><b>Menschliche Fehlhandlungen</b></p> <ul style="list-style-type: none"><li>- G 3.5 Unbeabsichtigte Leitungsbeschädigung</li><li>- G 3.85 Verletzung von Brandschottungen</li></ul> <p><b>Technisches Versagen</b></p> <ul style="list-style-type: none"><li>- G 4.6 Spannungsschwankungen/ Überspannung/Unterspannung</li><li>- G 4.62 Verwendung unzureichender Steckdosenleisten</li><li>- G 4.63 Verstaubte Lüfter</li></ul> <p><b>Vorsätzliche Handlungen</b></p> <ul style="list-style-type: none"><li>- G 5.8 Manipulation von Leitungen</li></ul>	<p><b>Infrastruktur</b></p> <ul style="list-style-type: none"><li>- M 1.3 Angepasste Aufteilung der Stromkreise</li><li>- M 1.5 Galvanische Trennung von Außenleitungen</li><li>- M 1.9 Brandabschottung von Trassen</li><li>- M 1.20 Auswahl geeigneter Kabeltypen unter physikalischen-mechanischer Sicht</li><li>- M 1.21 Ausreichende Trassendimensionierung</li><li>- M 1.22 Materielle Sicherung von Leitungen und Verteilern</li><li>- M 1.25 Überspannungsschutz</li><li>- M 1.64 Vermeidung elektrischer Zündquellen</li></ul> <p><b>Organisation</b></p> <ul style="list-style-type: none"><li>- M 2.19 Neutrale Dokumentation in den Verteilern</li><li>- M 2.391 Frühzeitige Information des Brandschutzbeauftragten</li><li>- M 2.394 Prüfung elektrischer Anlagen</li></ul> <p><b>Kommunikation</b></p> <ul style="list-style-type: none"><li>- M 5.1 Entfernung oder Deaktivierung nicht benötigter Leitungen</li><li>- M 5.4 Dokumentation und Kennzeichnung der Verkabelung</li><li>- M 5.5 Schadensmindernde Kabelführung</li></ul> <p><b>Notfallvorsorge</b></p> <ul style="list-style-type: none"><li>- M 6.18 Redundante Leitungsführung</li></ul>

# Der BSI-Sicherheitsprozess



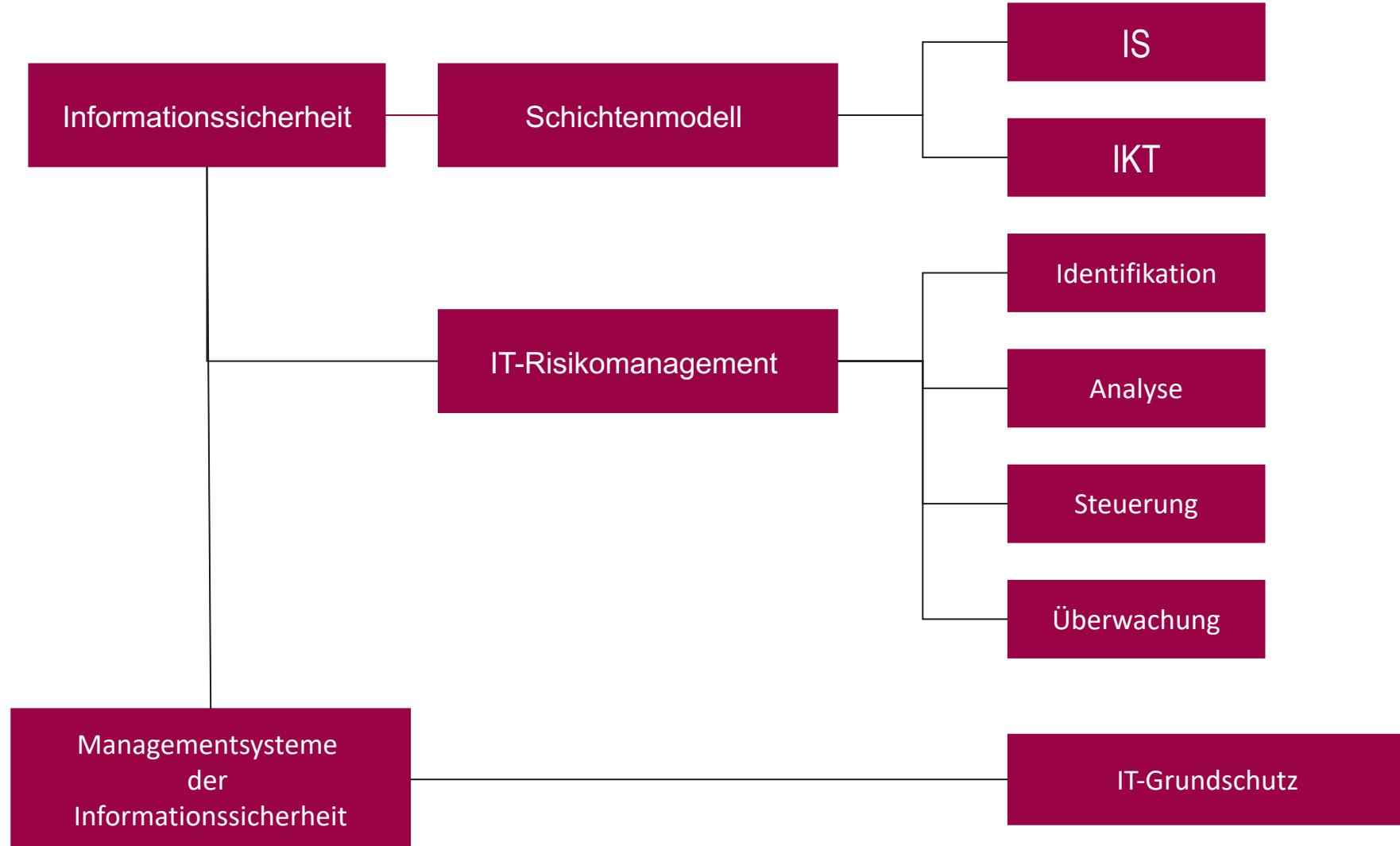
BSI-Standard 100-2

BSI-Standard 100-3

# Schweizer Sicherheitsvorgaben



# Begriffe zu LE10



Und nun sind Sie dran...





## Nach jeder Lerneinheit:

- Erstellen Sie Single Choice Aufgaben (Wahr/Falsch)

## Ablauf:

- Sie brauchen nur Zettel und Stift
- Alle erstellen 3 Wahr-Falsch-Aussagen (Lernziele!)
- Mit Nachbarn tauschen und gegenseitig beantworten / diskutieren
- Zum Schluss abgeben (idealerweise physisch, notfalls Mail)

## Ziel:

- Reflexion des theoretischen Inputs
- Anreicherung des Fundus an Klausuraufgaben

## Lernziele LE10



- 1) Sie sind vertraut mit dem Management und kennen wichtige **Standards** und **Rahmenwerke** zur **Informationssicherheit**.
- 2) Sie verstehen das **Ebenenmodell** der **Sicherung von Informationen** und kennen die **Risikomanagementprozesse** im Informationsmanagement.
- 3) Ihnen ist **IT-Grundschutz-Rahmenwerk** geläufig.

# Literatur

## Kernliteratur

- BSI (2006). IT-Sicherheitsmanagement und IT-Grundschutz. BSI-Standards zur IT-Sicherheit: Bundesanzeiger.
- Krcmar, H.: Informationsmanagement (2015), S. 563-590

## Vertiefungsliteratur

- Adams, J.(1995): Risk. London, UK: UCL Press
- Anderson, R. (2001): Security engineering: a guide to building dependable distributed systems. New York Wiley



## Prof. Dr. Matthias Söllner

Fragen zur Vorlesung können Sie gerne via Mail an [soellner@uni-kassel.de](mailto:soellner@uni-kassel.de) richten.

Weitere Informationen zum Fachgebiet finden Sie unter: [www.uni-kassel.de/go/wise](http://www.uni-kassel.de/go/wise)

