



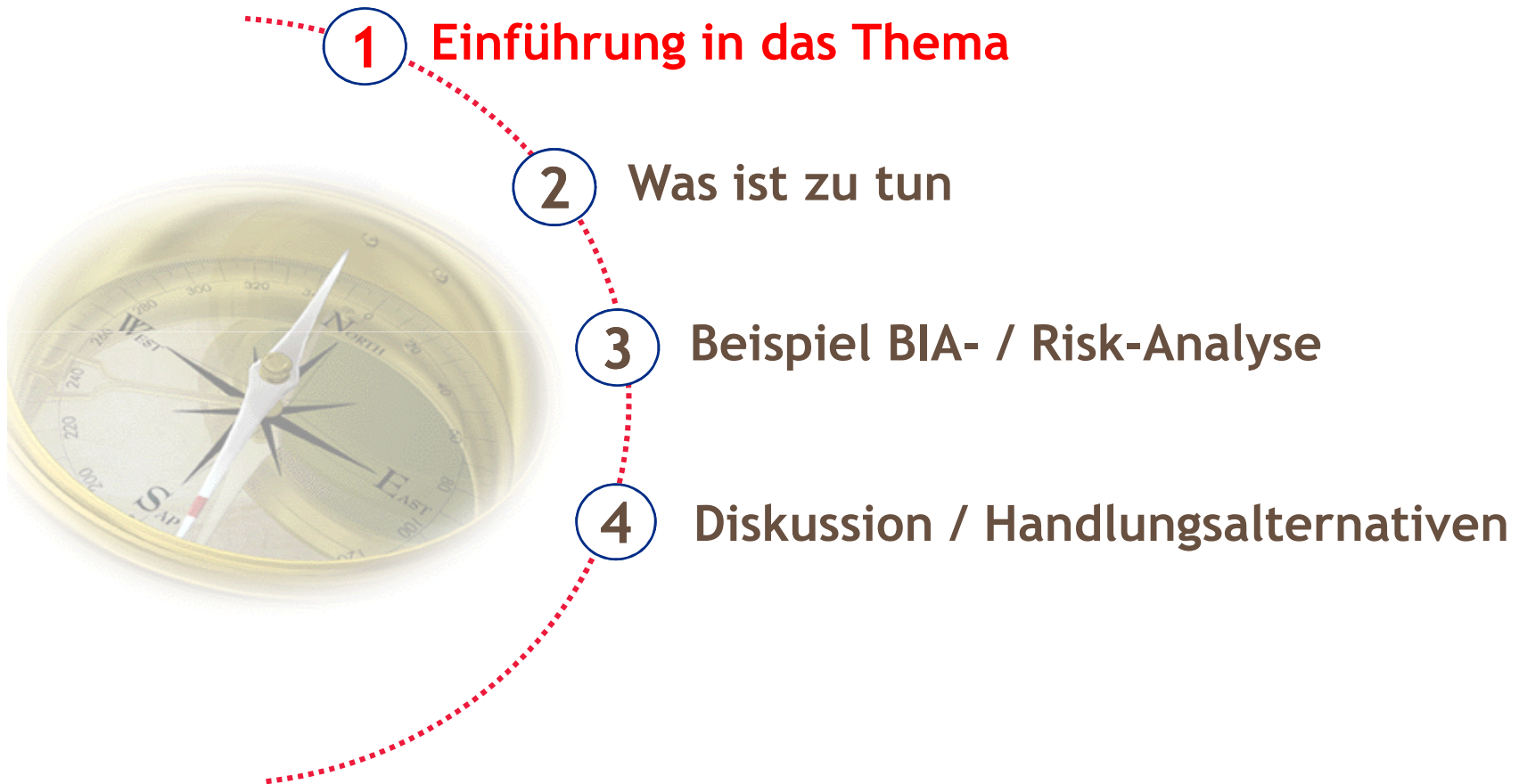
IT-NOTFALLKONZEPT

9. Fachtag IV / IT des BeB

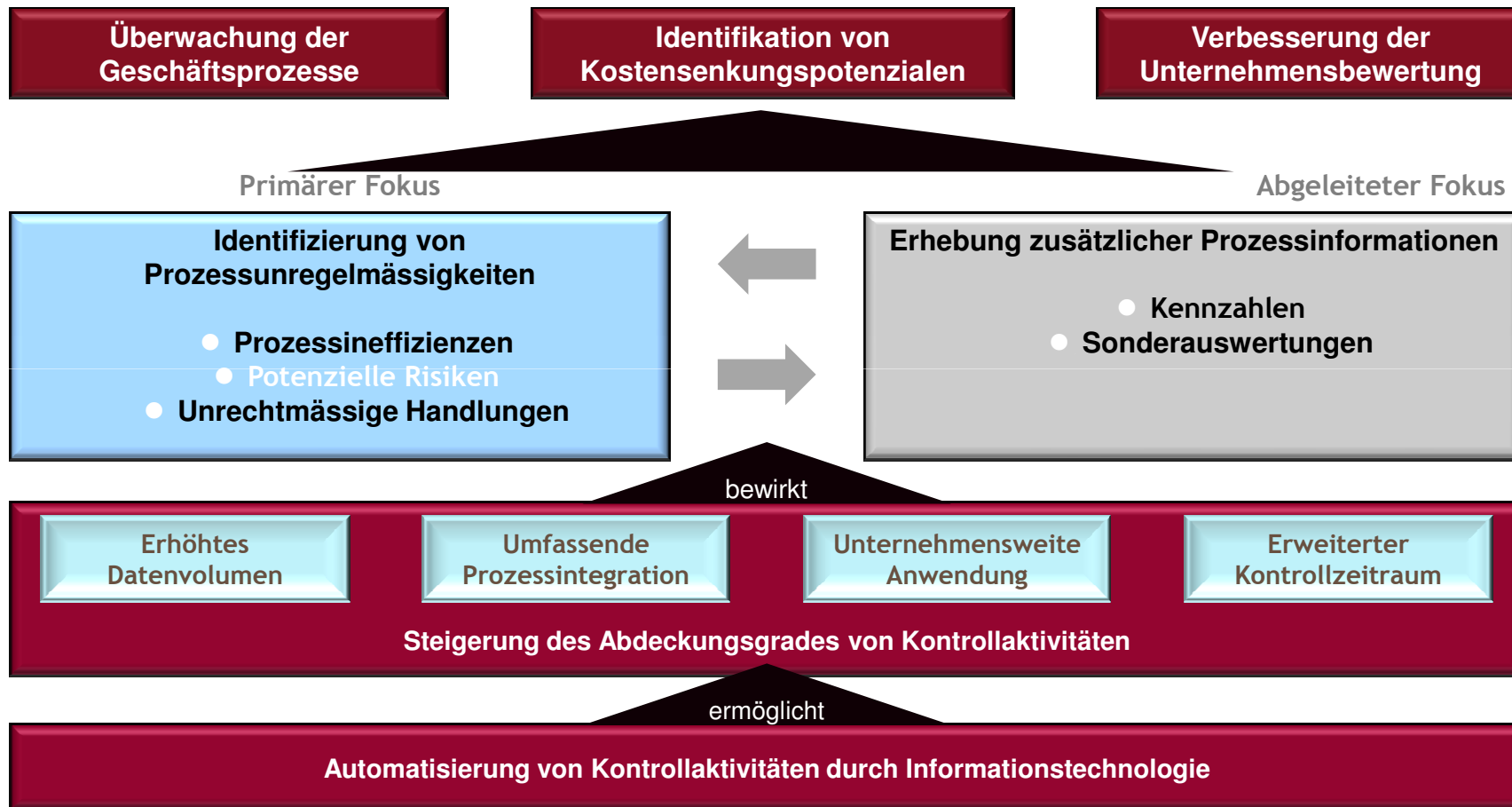
Fulda, 28. April 2010



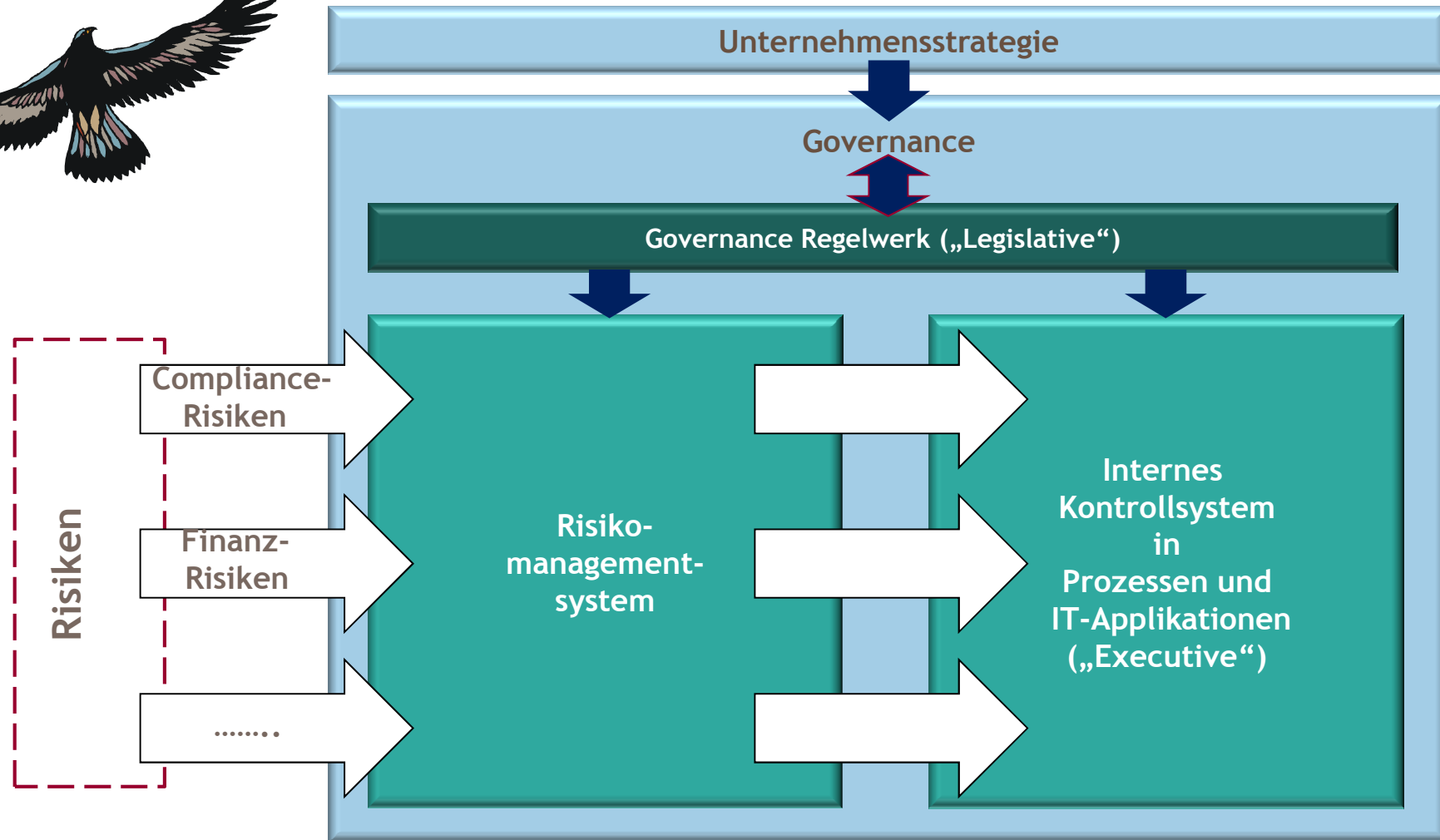
AGENDA



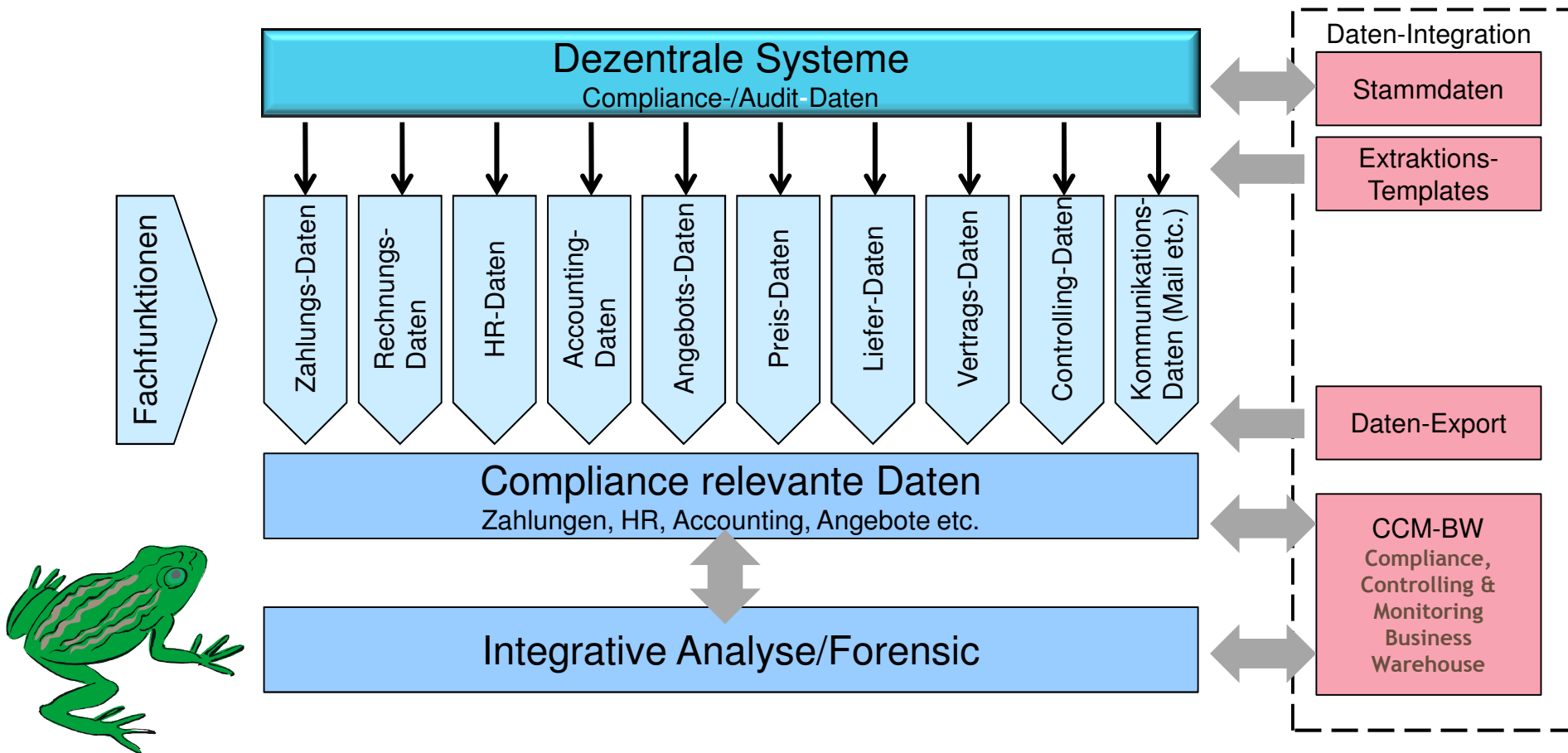
COMPLIANCE INTELLIGENCE ENTWICKLUNGSMODELL



COMPLIANCE-ORGANISATION - FRAMEWORK



VISION DER „DATENDREHSCHIBE“





NOTFALL POLICY - EINLEITUNG (BEISPIELDEFINITION)

Die Notfallpolicy enthält organisatorische Lösungsansätze und Vorsorgemaßnahmen, die bei der Bewältigung von internen und externen Risiken, die Geschäftstätigkeit der Einrichtung beeinträchtigen bzw. stören, unterstützen sollen. Die oberste Anforderung ist es, die Verfügbarkeit, Vertraulichkeit und Integrität der eigenen und der von den Kunden/Patienten und Geschäftspartnern anvertrauten Informationen und Ressourcen sicherzustellen. Die Nachvollziehbarkeit, Verbindlichkeit und Ordnungsmäßigkeit von Prozessen ist zu garantieren, um das Erreichen der Unternehmensziele zu gewährleisten und Schaden durch den Eintritt von unerwünschten Ereignissen (Risiken) zu verhindern bzw. zu begrenzen.

Oberste Zielsetzung ist es, den Fachbereichen eine funktionsfähige IT-Unterstützung (BCP) im Rahmen der Fachbereichsprozesse unter Berücksichtigung der definierten Ausfallzeiten (BIA) zur Verfügung zu stellen.



DEFINITIONEN - BETRIEBSSTÖRUNG VS. NOTFALL

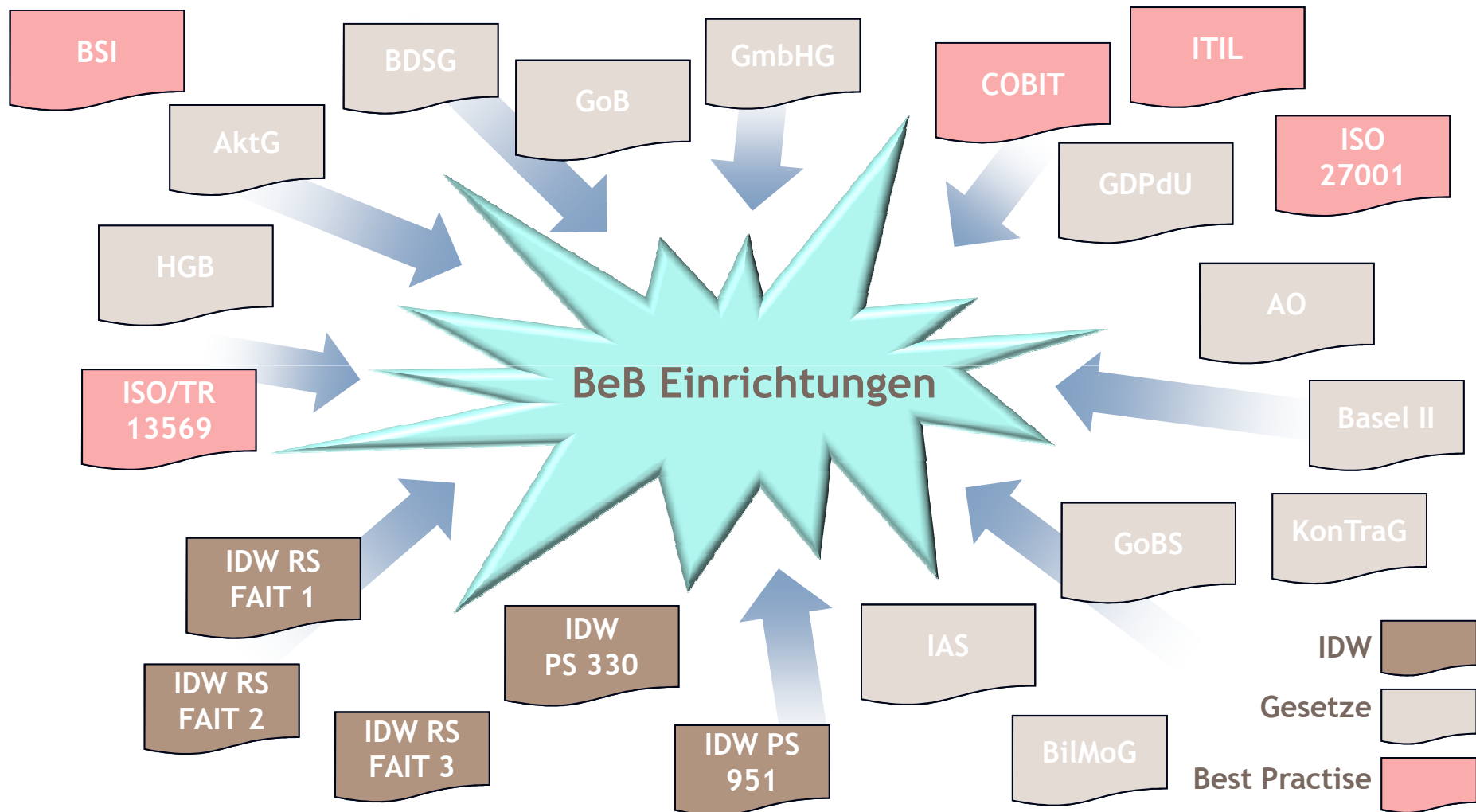
- Betriebsstörungen
 - Betreffen ein Störung des garantierten Online-Betriebes. Betriebsstörungen betreffen also den Ausfall einzelner Komponenten, Fehler in der Software oder im System Management, kurz: sie behandeln „die tägliche Katastrophe“, die in Ihrer Auswirkung jedoch lokal begrenzt ist und i.d.R. zeitnah behoben werden kann (geregelt im Sicherheitskonzept). Durch unzureichende Eskalation kann sich auch eine Betriebsstörung zu einem Notfall ausweiten.



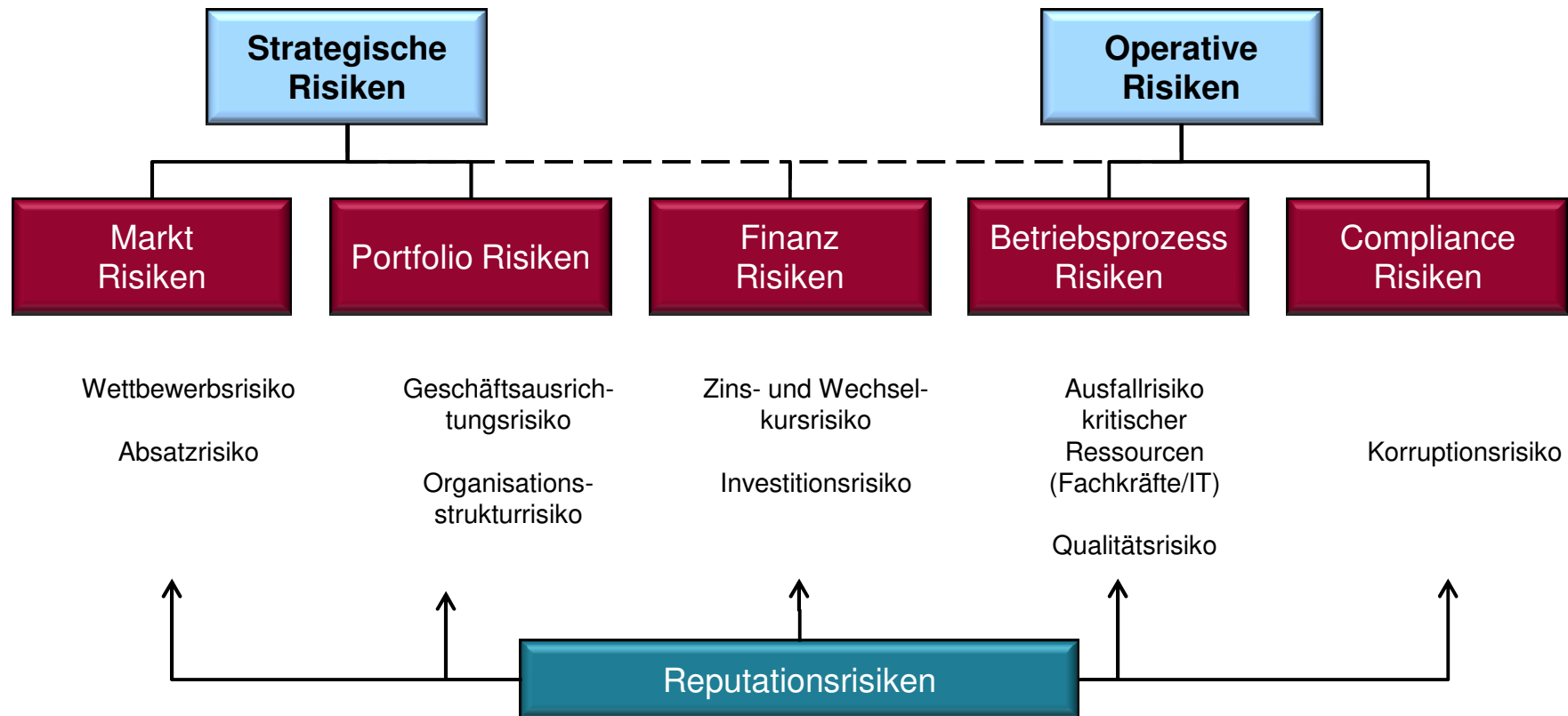
DEFINITIONEN - BETRIEBSSTÖRUNG VS. NOTFALL

- Notfall
 - Ein Notfall (Katastrophenfall) stellt eine Störung größeren Ausmaßes dar, also z. B. einen Ausfall des Rechenzentrums oder mehrerer kritischer „Single Points of Failures“ und ist dann gegeben, wenn in Frage gestellt ist, ob die IT-Umgebung (für kritische Anwendungen) innerhalb einer bestimmten maximalen Frist nach Eintritt der Störung wiederhergestellt werden kann.
 - Weiterhin können sich auch Ereignisse, die neben der Verfügbarkeit auch die Integrität und Vertraulichkeit der Daten beeinflussen, sich zu einem Notfall ausweiten (z. B. Kompromittierung von Daten durch Ausfall einer Firewall). Zum Notfall zählt auch der Ausfall eines Standortes z.B. durch Großbrand, Flugzeugabsturz etc. Die Auswirkungen dieser Szenarien betreffen mit hoher Wahrscheinlichkeit nicht nur die IT sondern hätten ein weiter reichende Schadensausmaß zur Folge.

EXTERNE/RECHTLICHE RAHMENBEDINGUNGEN



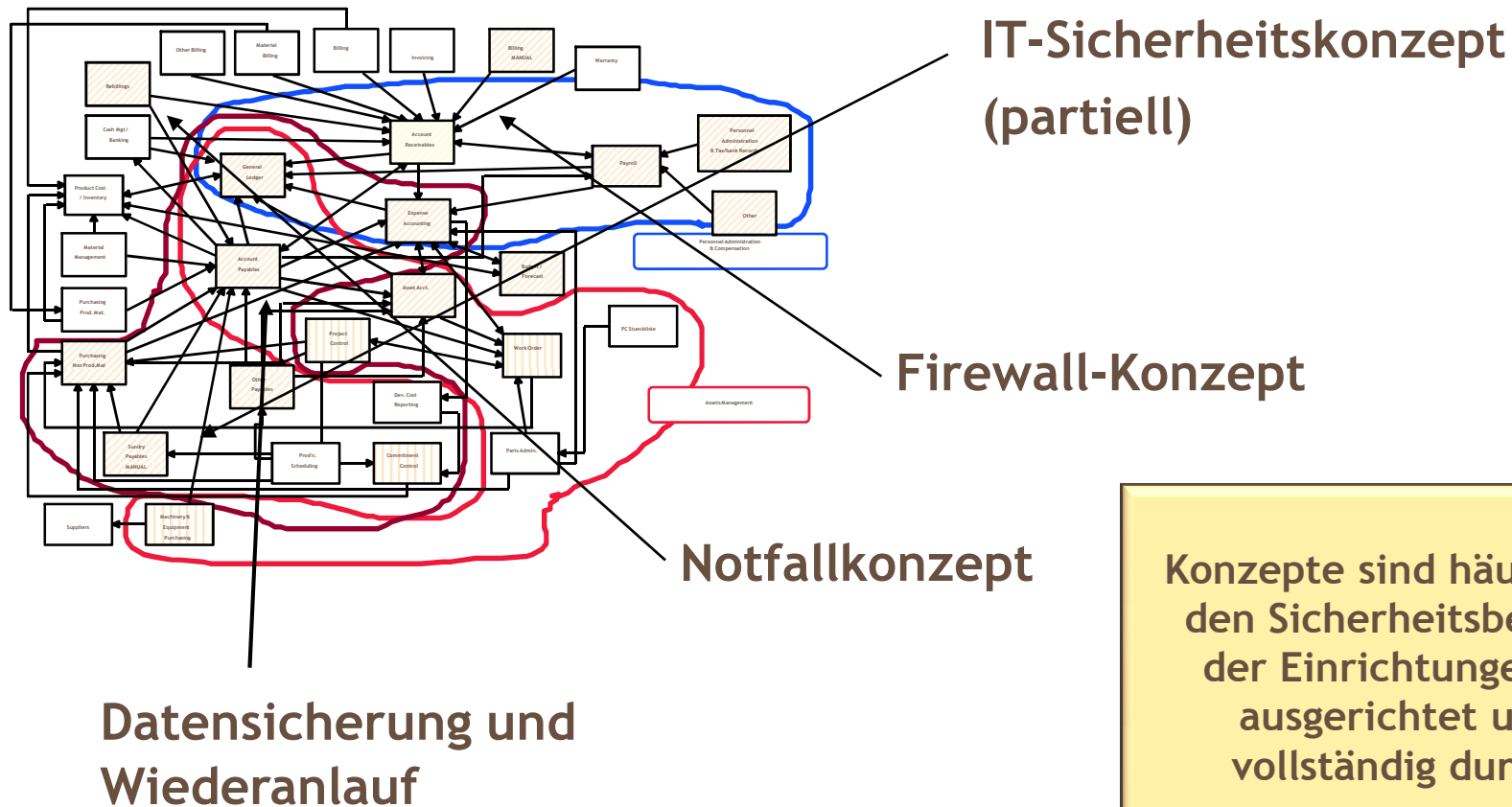
KATEGORIEN VON UNTERNEHMENSRIKIKEN



AGENDA

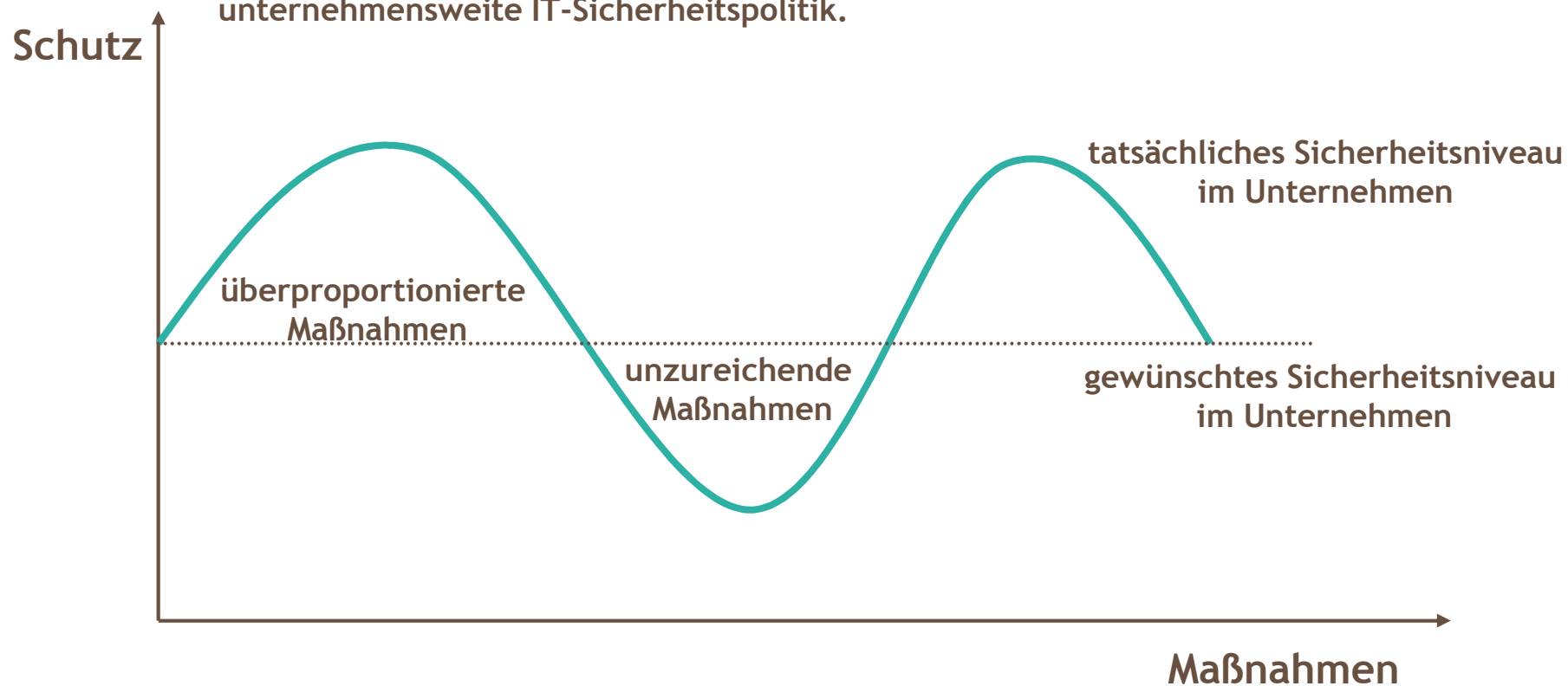


HÄUFIG WIRD EIN PRAGMATISCHEN ANSATZ GENUTZT!



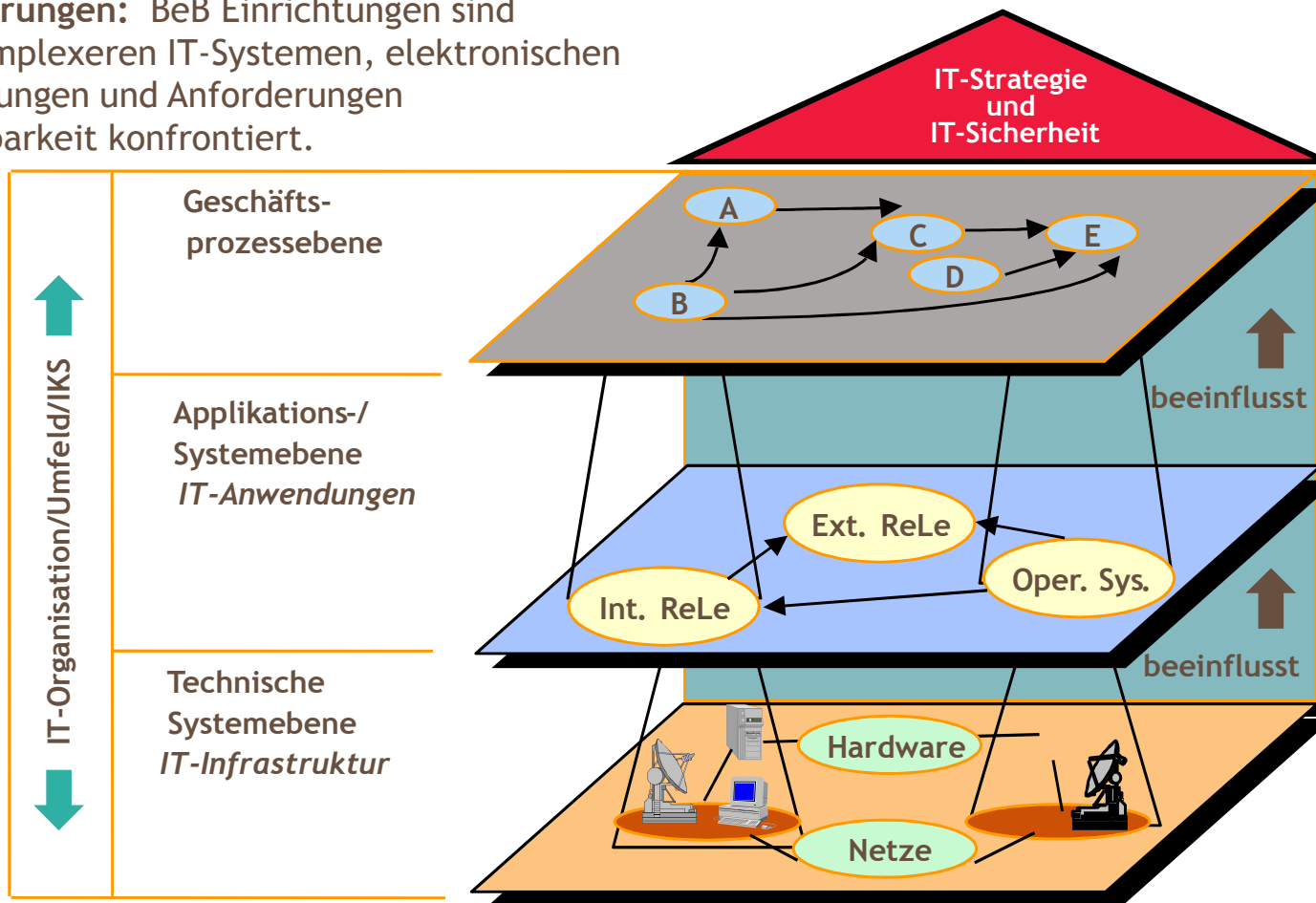
MAßNAHMENUMSETZUNG (WIRKSAMKEIT)

Trotz Umsetzung einzelner Maßnahmen verbleiben Lücken in der IT-Sicherheit, da ein unternehmensweites Vorgehen fehlt wie z. B. eine unternehmensweite IT-Sicherheitspolitik.



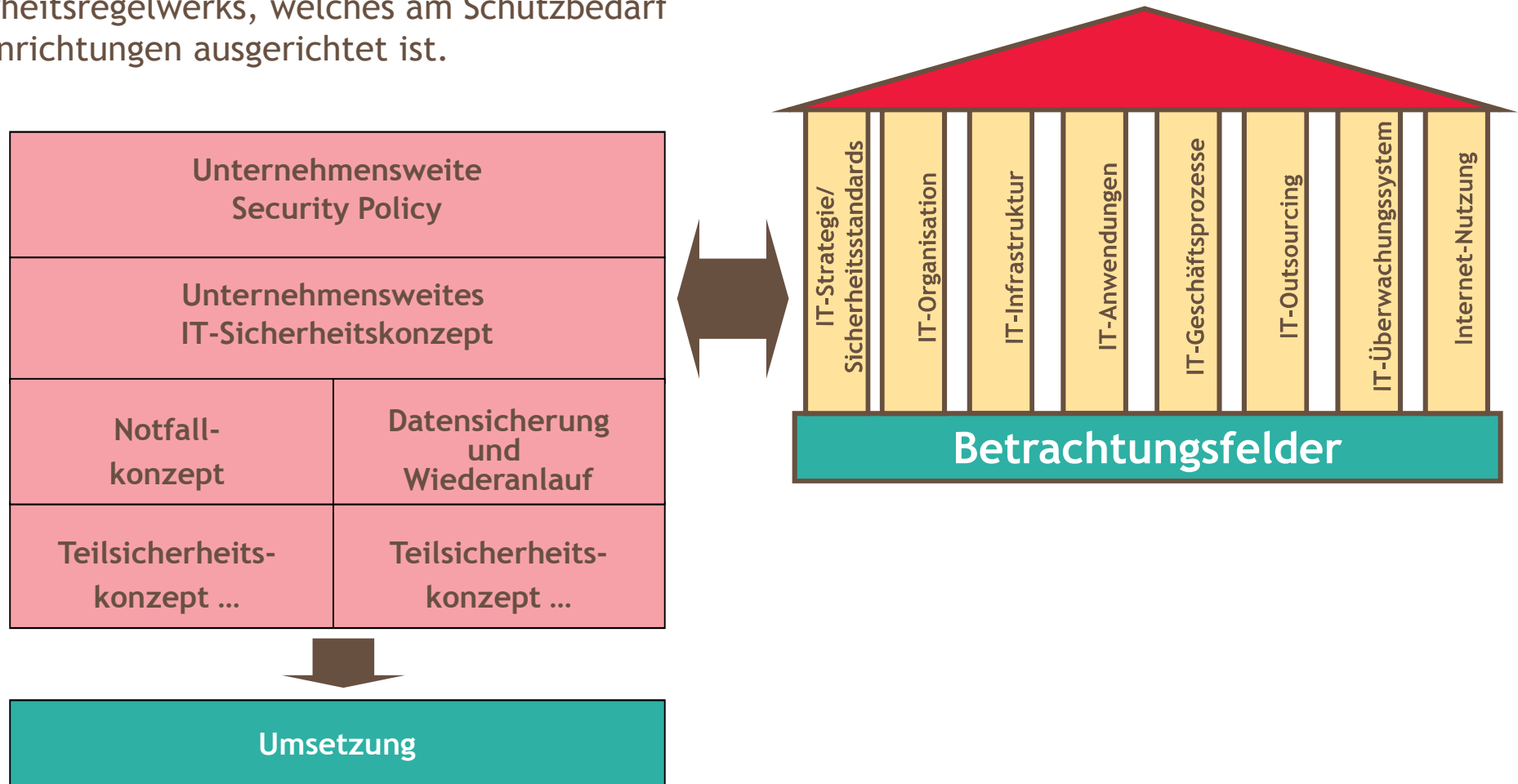
SICHERHEIT ERFORDERT GANZHEITLICHE BETRACHTUNG

Neue Anforderungen: BeB Einrichtungen sind mit immer komplexeren IT-Systemen, elektronischen Kundenbeziehungen und Anforderungen an die Verfügbarkeit konfrontiert.

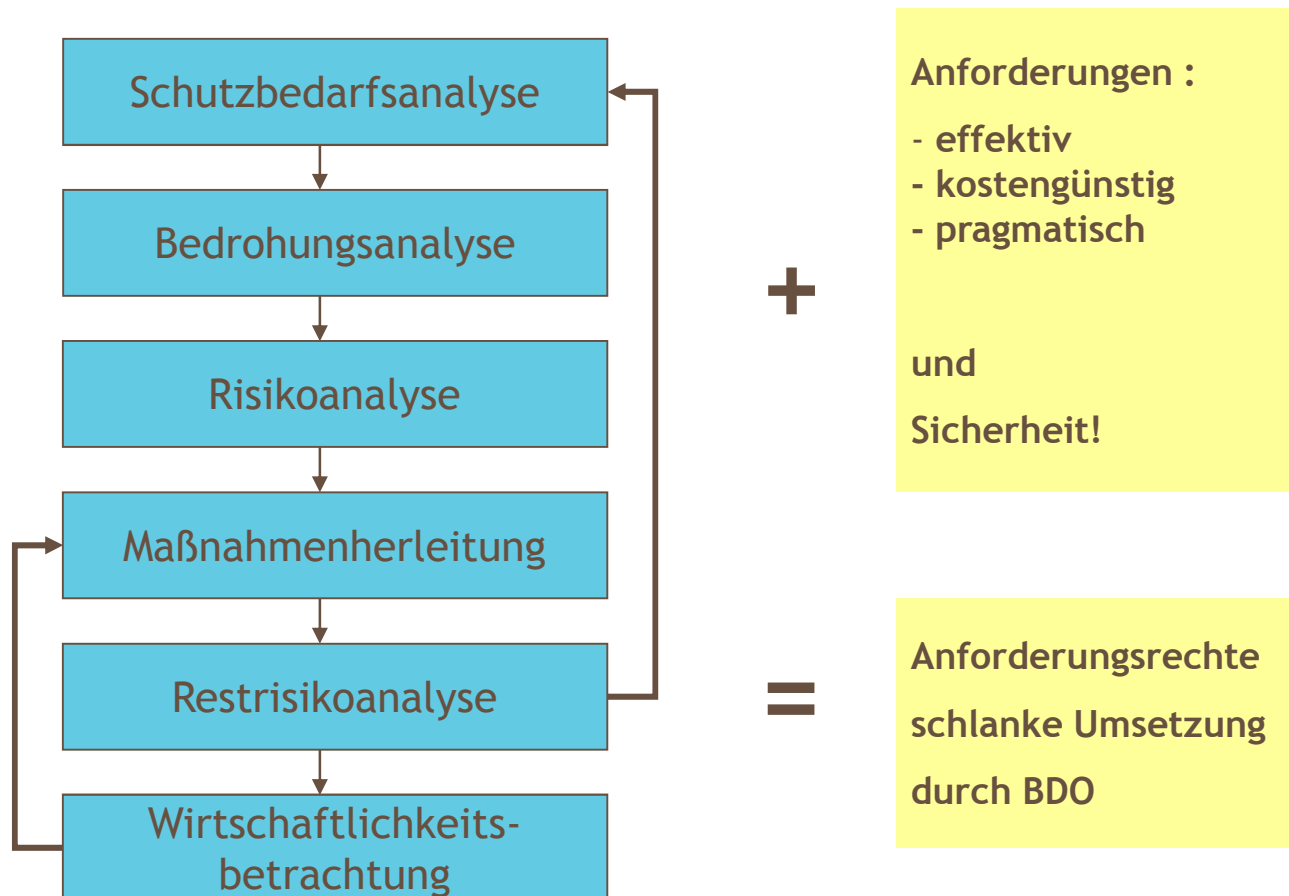


WAS IST ZU TUN ...

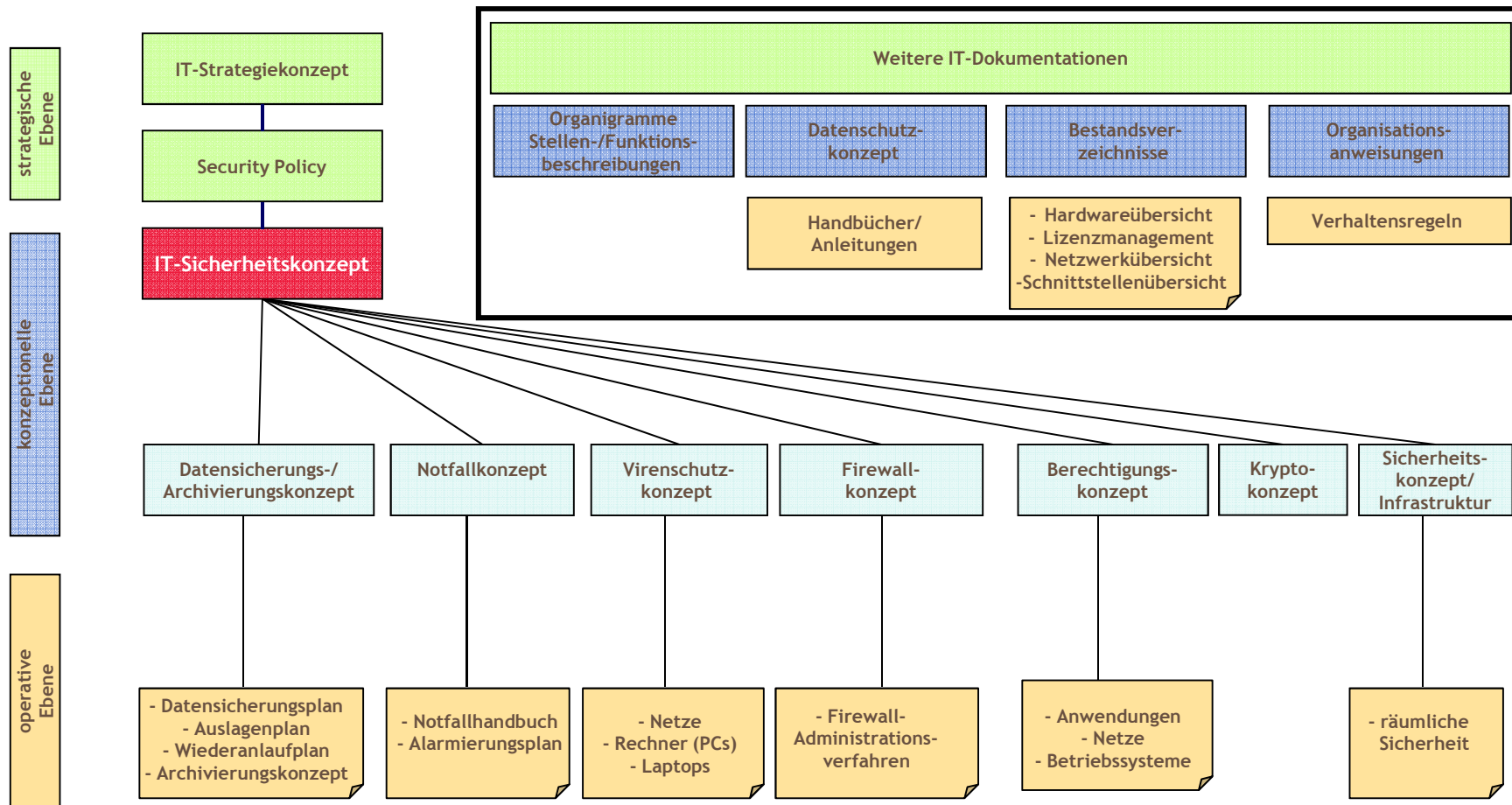
Einführung eines systematischen Sicherheitsregelwerks, welches am Schutzbedarf der Einrichtungen ausgerichtet ist.



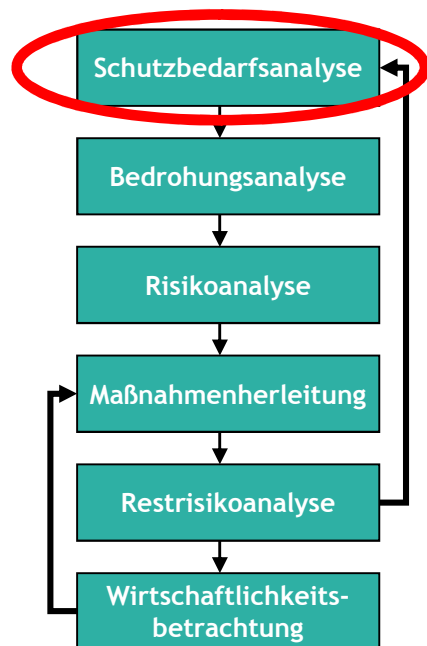
... UND WIE SOLLTE VORGEGANGEN WERDEN



EINFÜHRUNG: ÜBERSICHT DOKUMENTENINFRASTRUKTUR „IT-SICHERHEIT“



VORGEHENSWEISE



- Review der vorhandenen Dokumente
- Sammlung der Datentöpfe und relevanter Anwendungen
- Definition der Werteskalen
- Definition der Szenarien
- Durchführung des Schutzbedarfworkshops
- Abstimmung der Ergebnisse mit den Dateninhabern
- Abstimmung der Ergebnisse mit der Geschäftsführung



DEFINITIONEN: SCHUTZBEDARFSANALYSE

- Erfassung der IT-Anwendungen und zu verarbeitenden Informationen
- Bewertung hinsichtlich der drei Grundbedrohungen Verfügbarkeit, Integrität und Vertraulichkeit:
 - **Verfügbarkeit:**
Die Verfügbarkeit von Informationen/Daten liegt vor, wenn eine vorgegebene Funktionalität eines IT-Systems in der vorgesehenen Zeit erbracht werden kann und die Funktionalität des IT-Systems nicht vorübergehend bzw. dauerhaft beeinträchtigt ist.
 - **Integrität:**
Die Integrität von Informationen/Daten liegt dann vor, wenn Informationen/Daten nur von Befugten in vorgesehener Weise verarbeitet werden, so dass die Vollständigkeit, Korrektheit und Widerspruchsfreiheit gewährleistet ist.
 - **Vertraulichkeit:**
Die Vertraulichkeit von Daten/Informationen liegt dann vor, wenn Befugten die Informationen nur in der zulässigen Weise zugänglich sind und kein unbefugter Informationsgewinn stattfinden kann.



DEFINITIONEN: WERTESKALA

- Bewertung mit Hilfe einer 4-stufigen Werteskala (Größenordnung des Schadens)
 - 4: Existenzgefährdend
 - 3: Groß
 - 2: Mittel
 - 1: Gering
- Die Bedeutung der Werte muss für Schäden und andere Aspekte (z. B. Vertraulichkeitsstufen) definiert werden.



DEFINITIONEN: WERTESKALA VERFÜGBARKEIT

- Verfügbarkeit (maximal tolerierbare Ausfallzeit)

4:

3:

2:

1:

- Beispiel für eine Definition

4: halber Tag

3: 1-2 Tage

2: 1 Woche

1: >1 Woche



DEFINITIONEN: WERTESKALA INTEGRITÄT

- Integrität
 - 4:
 - 3:
 - 2:
 - 1:
- Beispiel für eine Definition
 - 4: Wiederherstellung nicht möglich
 - 3: Aufwand der Wiederherstellung zwischen 1 Tag und 1 Woche
 - 2: Aufwand der Wiederherstellung zwischen 1 Stunde und 1 Tag
 - 1: Kein Aufwand für die Wiederherstellung bzw. nicht notwendig



DEFINITIONEN: WERTESKALA VERTRAULICHKEIT (1/2)

- Vertraulichkeit
 - 4:
 - 3:
 - 2:
 - 1:
- Beispiel für eine Definition
 - 4: geheime Daten
 - 3: personenbezogene/gesetzliche Daten/Patientendaten
 - 2: unternehmensinterne Daten
 - 1: öffentliche/informelle Daten

DEFINITIONEN: WERTESKALA VERTRAULICHKEIT (2/2)

- **Klasse 1: Öffentliche/informelle Daten**
Darunter sind Daten klassifiziert, deren Offenlegung oder Veränderung/Verfälschung keinen oder nur einen unbedeutenden Schaden für das Unternehmen darstellt und höchstens einen finanziellen Verlust von XX € beziffert. Ein Imageverlust ist mit der Schädigung nicht verbunden.
- **Klasse 2: Unternehmensinterne Daten**
Daten dieser Klasse dürfen keiner Veränderung/Verfälschung unterliegen. Der finanzielle Verlust hält sich in Grenzen (XX-YY €), der Imageschaden ist gering. Die Daten sollten nur unternehmensintern zugänglich sein. stehen.
- **Klasse 3: Personenbezogene/gesetzliche Daten / Patientendaten**
Daten der Klasse 3 sind Daten, deren Schutz durch gesetzliche Auflagen vorgeschrieben ist, wie BDSG, GoBS, AO, KonTraG etc. Dazu gehören personenbezogene Daten, wie sie z. B. in der Personalabteilung verarbeitet werden. Eine Offenlegung oder unbefugte Veränderung bzw. Verfälschung stellt mittleren Schaden für das Unternehmen dar und höchstens einen finanziellen Verlust von XX €. Ein Imageverlust ist mit der Schädigung verbunden.
- **Klasse 4: Geheime Daten**
Daten der Klasse 4 sind strategische Planungsdaten des Unternehmens. Eine Offenlegung oder unbefugte Veränderung bzw. Verfälschung stellt einen hohen Schaden für das Unternehmen dar, ist mit einem finanziellen Verlust von mehr als XX € verbunden und kann existenzgefährdend sein. Ein großer Imageverlust ist mit der Schädigung zwingend verbunden.



SCHUTZBEDARFSANALYSE: DARSTELLUNG DER SZENARIEN

Zur besseren Bewertung der Daten und Anwendungen könnten zum Beispiel folgende Szenarien verwendet werden:

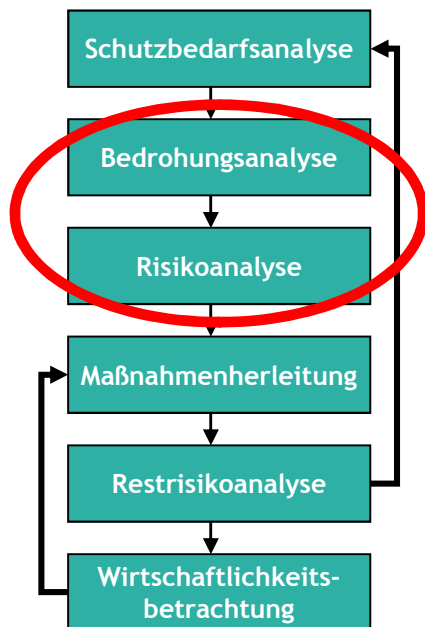
- **Verarbeitungsfehler**
Der aufgetretene Fehler wird durch ein maschinellen oder personellen Verarbeitungsfehler verursacht. Im Normalfall ist so ein Fehler durch die IT-Abteilung selbst behebbar.
- **Hardwarefehler**
Beispiele für Hardwarefehler sind defekte Festplatten, defekter Prozessor oder Controller. In den meisten Fällen benötigt man zur Behebung des Fehlers Hilfe durch einen Dritten.
- **Worst Case**
Worst Case stellt den Notfall in einem Unternehmen oder in der IT-Abteilung dar. Dies wird explizit im Notfallkonzept geregelt.



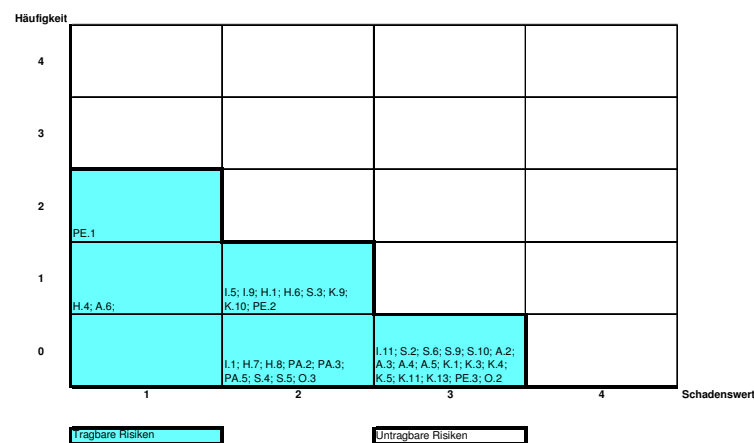
SCHUTZBEDARFSANALYSE: DATEN/ANWENDUNGEN

Szenario „Normalfall“				
Nummer	Bezeichnung der Anwendung oder Information	Wert der Verfügbarkeit	Wert der Integrität	Wert der Vertraulichkeit
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				

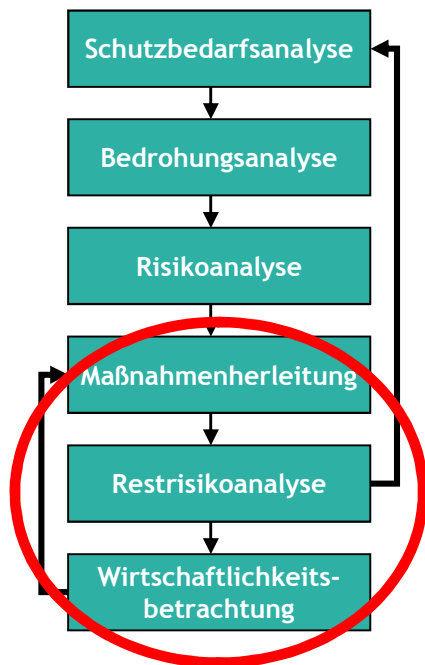
WEITERE VORGEHENSWEISE (1/3)



- Feststellung der relevanten Anwendungen
- Feststellung der betreffenden Hardware und Infrastruktur
- Definition der Gefährdungskataloge
- Beurteilung der Eintrittswahrscheinlichkeiten
- Ergebnis:



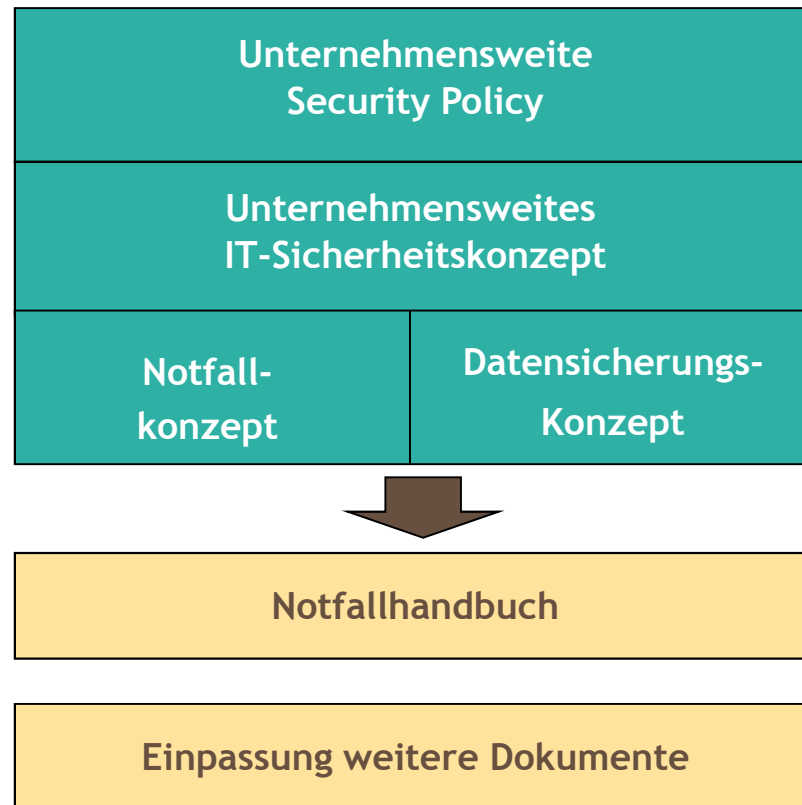
WEITERE VORGEHENSWEISE (2/3)



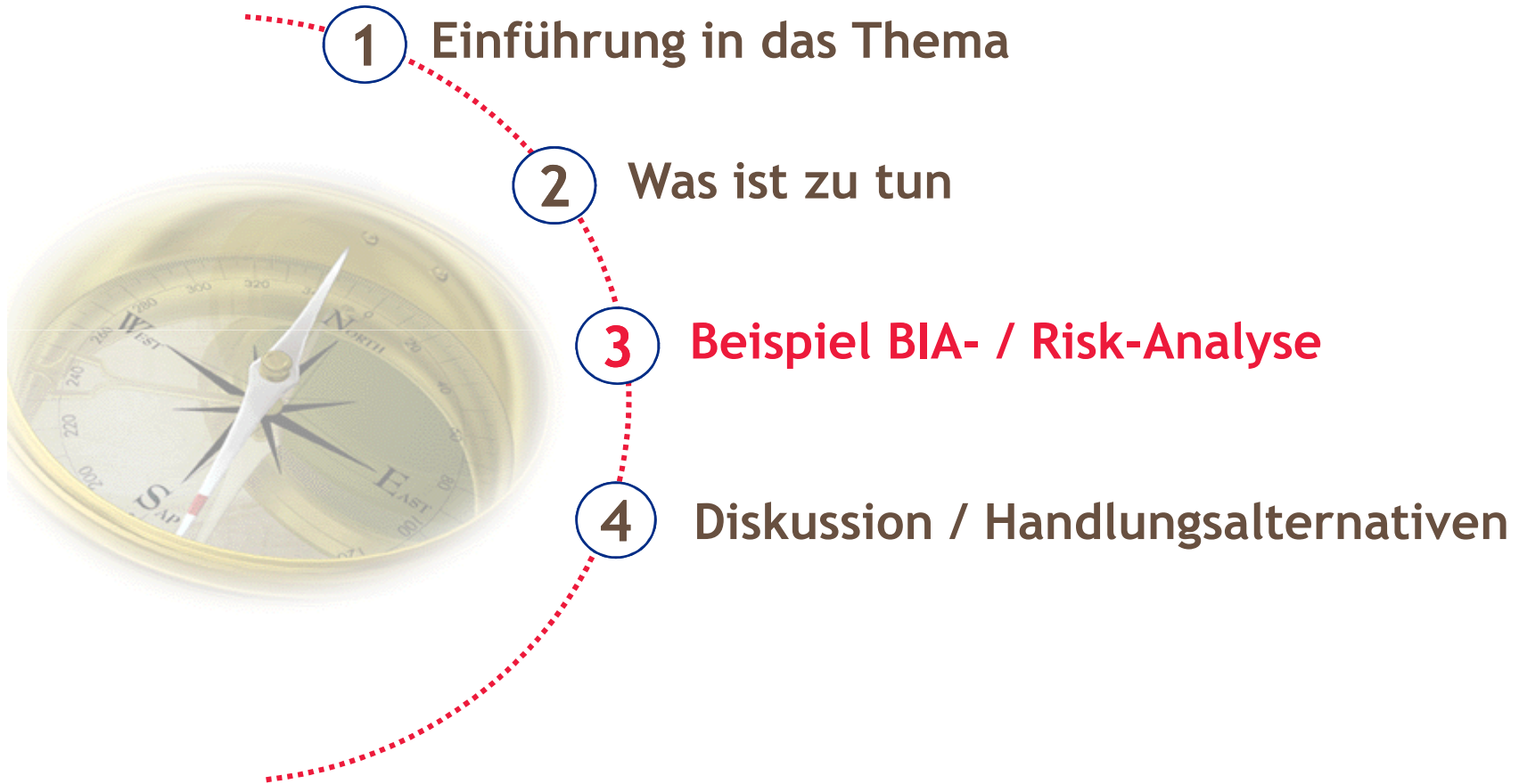
- Definition von Maßnahmenkatalogen
- Konsolidierung der Maßnahmen
- Feststellung des Restrisikopotenzials
- Definition der umzusetzenden Maßnahmen
- Betrachtung der Wirtschaftlichkeit

- Ergebnis:
 - Abgestimmter Maßnahmenkatalog

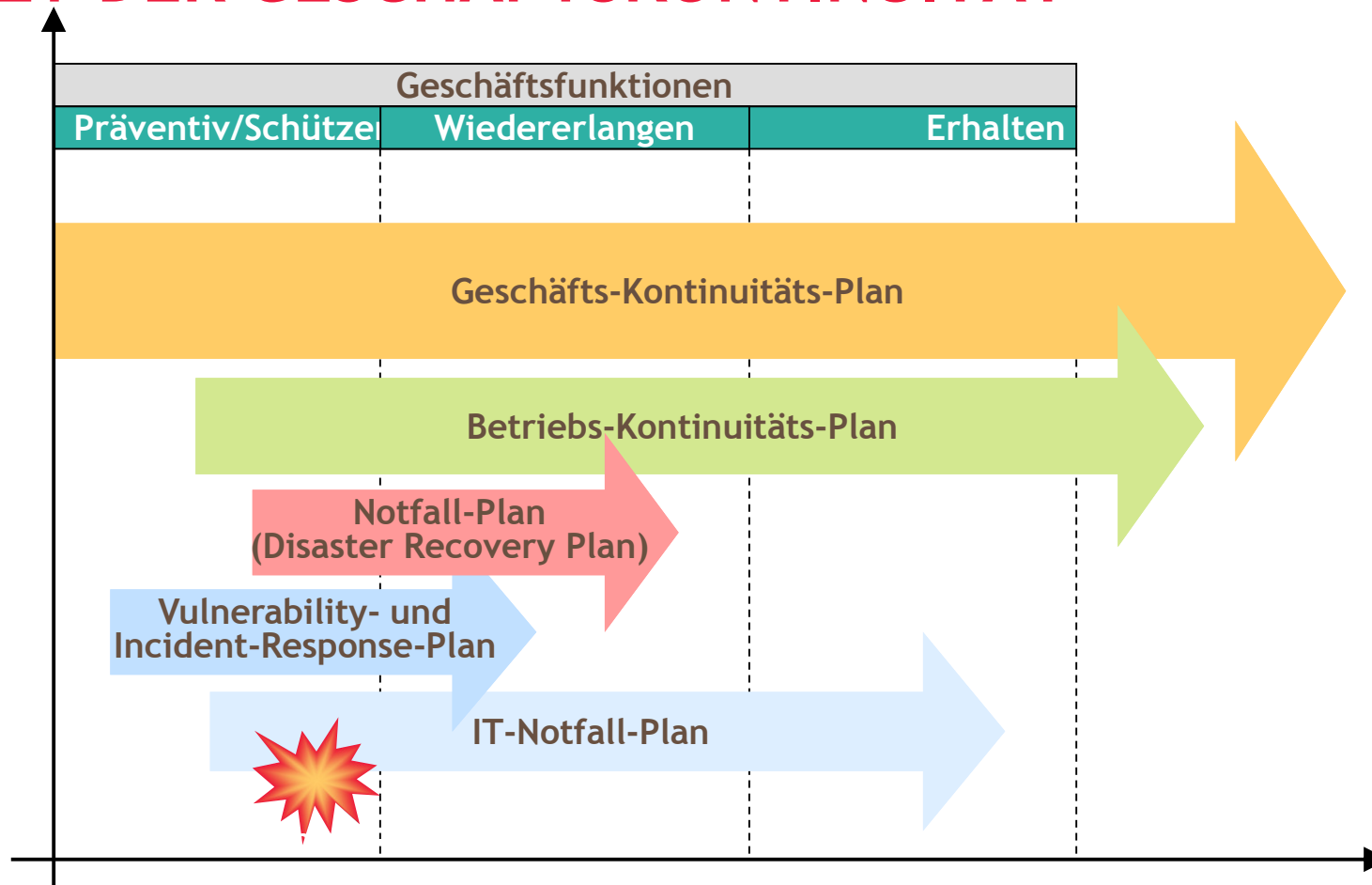
WEITERE VORGEHENSWEISE (3/3)



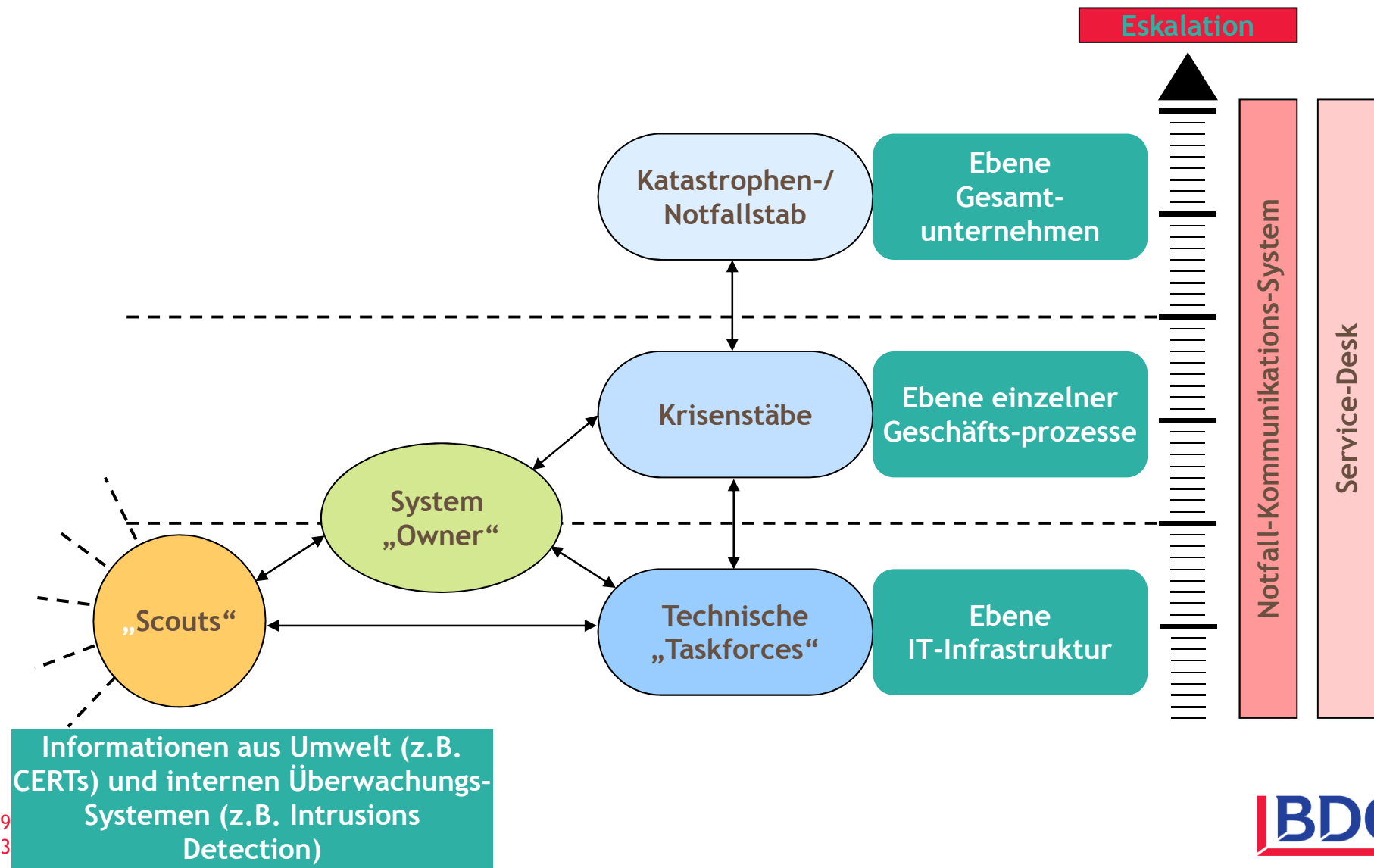
AGENDA



PLÄNE ZUM SCHUTZ, ZUR WIEDERERLANGUNG UND ZUM ERHALT DER GESCHÄFTSKONTINUITÄT



ESKALATIONS-EBENEN DER NOTFALL-PLANUNG



AGENDA



DANKE FÜR IHRE AUFMERKSAMKEIT



PRÄSENTIERT VON



BDO Deutsche Warentreuhand
Aktiengesellschaft
Wirtschaftsprüfungsgesellschaft

Berliner Allee 59 • 40212 Düsseldorf
Tel.: +49 211 1371-146 Fax: +49 211 1371-150
E-Mail: dieter.hefner@bdo.de
Internet: www.bdo.de

Diplom-Betriebswirt (FH)

Dieter Hefner

Partner

IT-Audit

Weltweit BDO International