Advisory

BCI Forum Mitte
Einführung in die „Business Impact Analyse“

Matthias Hämmerle MBCI

Frankfurt

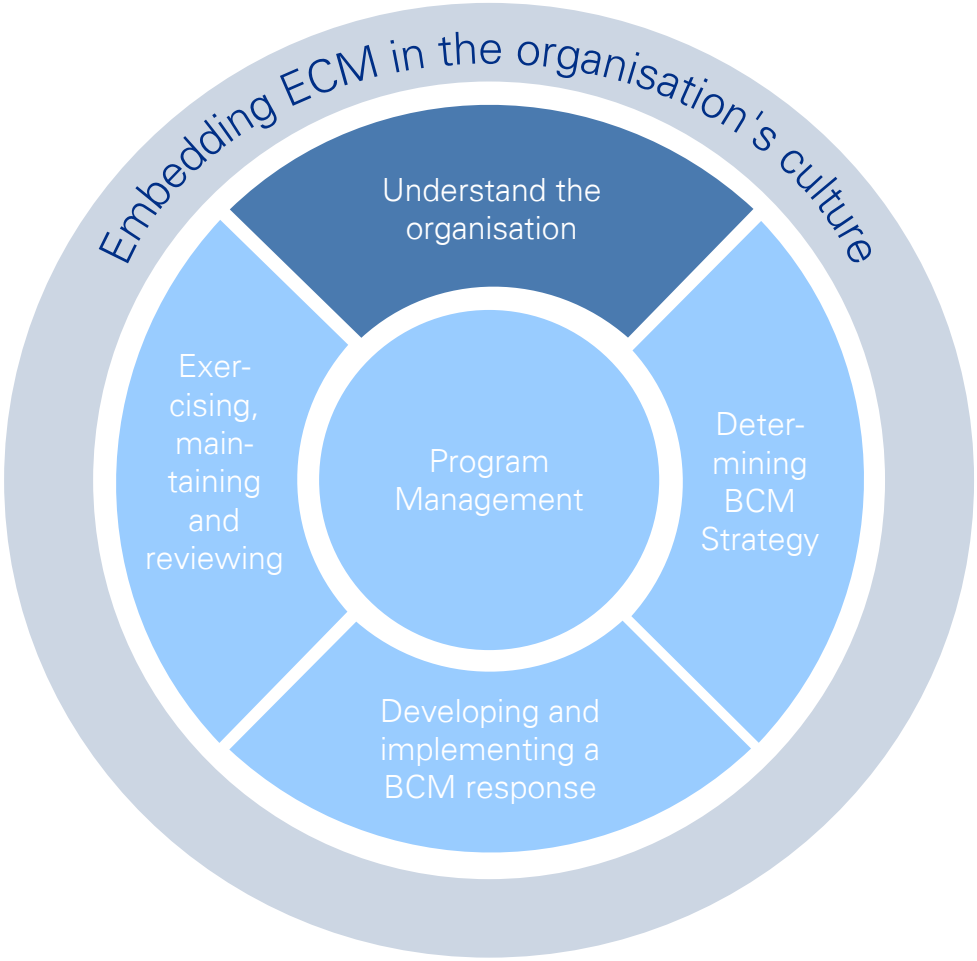
25. März 2008

AGENDA

Inhalt

- **Die Business Impact Analyse im BCI GPG und BS 25999**
- **Best Practices und Stolperfallen**
- **Diskussion**

Die Business Impact Analyse ist ein zentraler Bestandteil des BCM Lifecycles



„Understanding the Organisation“

Das „Verständnis des Geschäfts“ ist ein zentraler Baustein des BCM
Ziel ist

- Die zentralen Produkte und Services einer Organisation zu identifizieren
- Die (Zeit-) Kritikalität der notwendigen Prozesse zu definieren

Die Phase besteht aus den Bausteinen

1. Business Impact Analyse
2. Ermittlung von Verfügbarkeitsanforderungen
3. Risk Assessment

Im Rahmen der BIA werden die Schadenswirkungen des Ausfalls kritischer Geschäftsprozesse ermittelt

Ziele

- Identifikation der geschäftskritischen Prozesse und ihre Anforderungen / Ressourcen
- Ermittlung der Auswirkungen einer Unterbrechung oder Ausfall eines Geschäftsprozesses über die Zeit
- Identifikation der internen und externen Abhängigkeiten, die für das Funktionieren der Prozesse notwendig sind

Vorgehensweise

- Identifikation der Prozesse und Prozessverantwortliche
- Identifikation der Ansprechpartner
- Identifikation der Impact-Kategorien (Finanziell, Reputation etc.)
- Festlegung des zu betrachtenden Zeithorizonts für die Schadensbeurteilung
- Risikobeurteilung: Festlegung des Risikoraums
  - Für Standorte, Märkte
  - Rechtliche Einheiten
  - Produkte

Ergebnisse

- Auswirkungen bei Unterbrechung oder Ausfall („Impact“)
- „Maximum Tolerable Period of Disruption MTPD“ für jeden Prozess
  - Wiederanlaufzeit
  - Notbetrieb
  - Rückkehr in den Normalbetrieb
- „Recovery Point Objective RPO“: Zeitpunkt, zu dem Informationen für die Prozesse wiederhergestellt sein müssen
- Geschäftskritische Prozesse und Ressourcen

Die BIA sollte mindestens einmal jährlich überprüft werden

Methoden

- Workshops
- Questionnaires: papiergestützt oder software – gestützt
- Interviews: strukturiert oder unstrukturiert

Review

- Die Business Impact Analyse sollte im Minimum einmal jährlich überprüft werden
- Eine häufigere Überprüfung sollte durchgeführt werden, wenn
  - Sich das Geschäft sehr stark und schnell ändert
  - Sich interne Prozesse, Standorte oder Technologie ändern
  - Sich starke Änderungen im externen Geschäftsumfeld (Markt, regulatorische Rahmenbedingungen etc.) ergeben.

Die MaRisk fordern von Finanzdienstleistern die Identifikation zeitkritischer Aktivitäten und Prozesse

- **Mindestanforderungen für das Risikomanagement (MaRisk)**
  - AT 7.3 Abs. 1 Notfallkonzept

    „Für Notfälle in **zeitkritischen Aktivitäten und Prozessen** ist Vorsorge zu treffen (Notfallkonzept). Die im Notfallkonzept festgelegten Maßnahmen müssen dazu geeignet sein, das Ausmaß möglicher Schäden zu reduzieren. Die Wirksamkeit und Angemessenheit des Notfallkonzeptes ist regelmäßig durch Notfalltests zu überprüfen. Die Ergebnisse der Notfalltests sind den jeweiligen Verantwortlichen mitzuteilen. Im Fall der Auslagerung von zeitkritischen Aktivitäten und Prozessen haben das auslagernde Institut und das Auslagerungsunternehmen über aufeinander abgestimmte Notfallkonzepte zu verfügen. “

  - AT 7.3 Abs. 2 Notfallkonzept

    „Das Notfallkonzept muss Geschäftsfortführungs- sowie Wiederanlaufpläne umfassen. Die Geschäftsfortführungspläne müssen gewährleisten, dass im Notfall zeitnah Ersatzlösungen zur Verfügung stehen. Die Wiederanlaufpläne müssen innerhalb eines angemessenen Zeitraums die Rückkehr zum Normalbetrieb ermöglichen. Die im Notfall zu verwendenden Kommunikationswege sind festzulegen.

    „Das Notfallkonzept muss den beteiligten Mitarbeitern zur Verfügung stehen.“

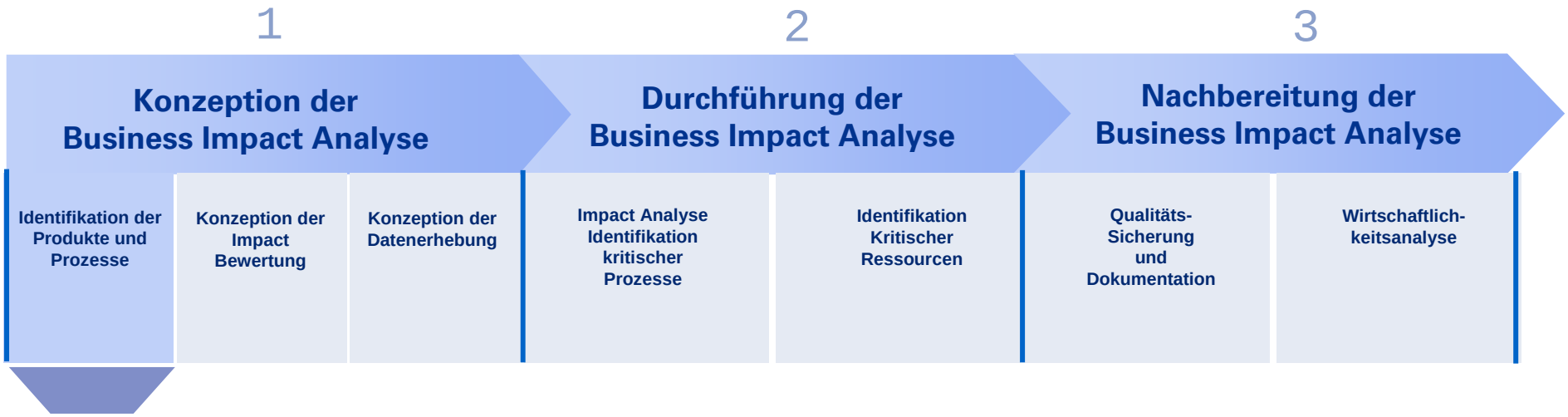
Die MARisk für Versicherungen liegen im Entwurf vor:
Analog zu den Banken forden die MaRisk für Versicherungen die Implementierung eines Notfallkonzepts.

AGENDA

Inhalt

- **Die Business Impact Analyse im BCI GPG und BS 25999**
- **Best Practices und Stolperfallen**
- **Diskussion**

Ein Best Practice Ansatz für die Durchführung einer Business Impact Analyse



Phase	Inhalt
Identifikation der Produkte und Prozesse	• Abgrenzung der relevanten Organisationsbereiche • Sammlung und Auswertung vorhandener Prozessdaten Ergebnisse: • Definierter und freigegebener Scope für die BIA • Prozesskatalog als Grundlage für die BIA

Die BIA basiert auf dem Geschäftsprozessmodell der Organisation

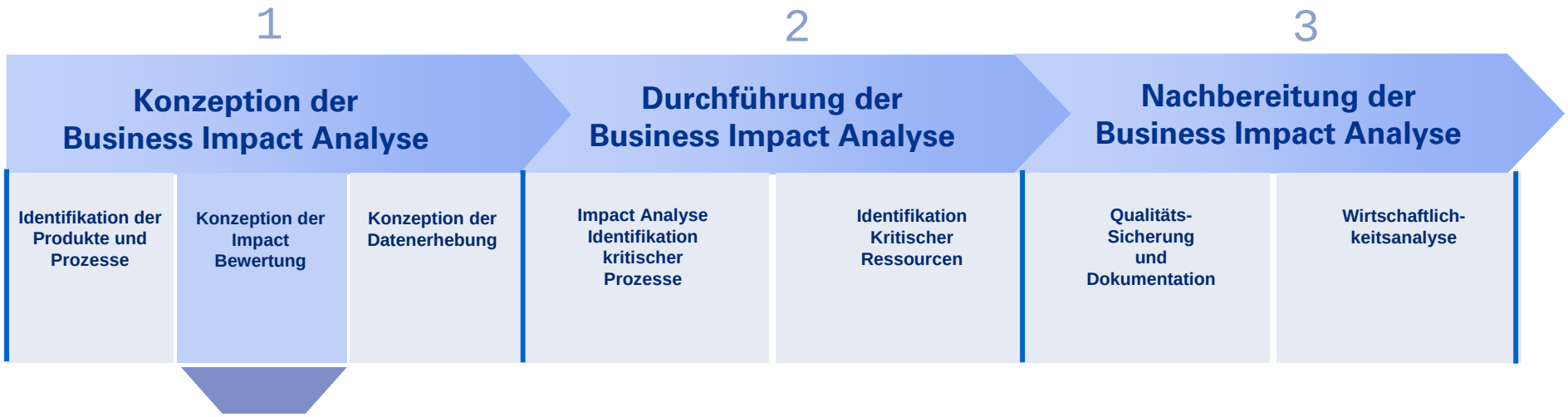
Abgrenzung relevanter Organisationsbereiche

- Gibt es Organisationsbereiche, die von der BIA ausgenommen werden sollen?
  - Bereiche wurden vom Management als nicht kritisch eingestuft
  - Für bestimmte Unternehmensbereiche wird zum Beispiel auf Grund der Größe oder der Relevanz für das Unternehmensrisiko keine BIA durchgeführt

Sammlung und Auswertung von Prozess-daten

- Die BIA basiert auf vorhandenen Prozessinformationen
- Sind die Prozessinformationen nicht vorhanden oder nicht aktuell, sind diese in einem gesonderten Projekt zu erheben
- Ziel der BIA ist es nicht Prozesse zu modellieren!
- Nicht im Detail verlieren: je Bereich 10-15 Prozesse (Faustformel)
- Denken Sie daran, daß die erhobenen Daten später auch gepflegt werden müssen

Das Impact-Bewertungsmodell ist das methodische Kernelement der BIA



Phase	Inhalt
Konzeption der Impact Bewertung	• Festlegung der Impact Kategorien (Finanzielle Schäden, Reputation, Rechtliche und Regulatorische Rahmenbedingungen, Steuerungsfähigkeit, Gefährdung der Gesundheit von Personen) • Festlegung der Betrachtungshorizonte für die Impact Bewertung • Festlegung der Risikoakzeptanzniveaus durch das Top-Management (ex ante) Ergebnisse: • Definierter Maßstab zur Impact-Bewertung und Festlegung der Kritikalität von Prozessen

Die BIA basiert auf dem Geschäftsprozessmodell der Organisation

Festlegung der Impact Kategorien

- Bei der Impact Analyse wird auf die Auswirkungen einer Unterbrechung abgehoben, nicht auf die Ursachen
- Kategorien für Auswirkungen sind beispielhaft:
  - Finanzielle Auswirkungen
  - Reputationsschaden
  - Verstoß gegen gesetzliche oder regulatorische Bestimmungen
  - Verlust der Steuerungsfähigkeit
  - Sicherheit und Schutz von Personen
- Die Auswirkungskategorien sollten sorgfältig beschrieben sein. Beispielsweise welche Schäden als finanzielle Schäden einzubeziehen sind

Festlegung des Zeit-Horizonts

- Welcher Zeithorizont soll bei der Impact-Beurteilung zu Grunde gelegt werden?
- Die Skalierung ist abhängig von den typischen Schadensverläufen der Geschäftsprozesse (Handelsgeschäfte vs. Versicherungsgeschäfte)

Die Prozesse lassen sich abhängig von der Bewertung der Impacts in Portfolien gruppieren

Definition der kritischen Impact -Kategorien Beispiele:

Personenschäden:

Gefährdung der Gesundheit von Mitarbeitern, Kunden, Anwohnern etc.

Finanzielle Schäden:

Finanzielle Schaden, die mit einem Ausfall des Geschäftsprozesses verbunden sind.
Beispiele hierfür: Entgangene Umsätze, Personalkosten, Schadensersatzzahlungen, Zinsverlust, etc.

Image-, Reputationsschäden:

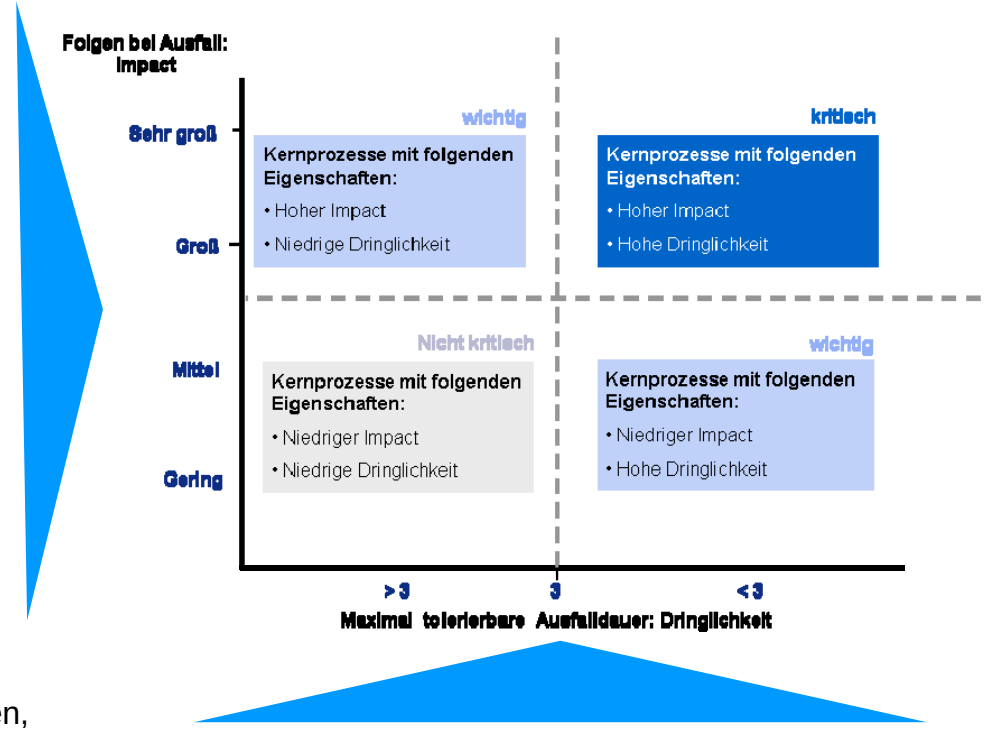
Das Unternehmen erleidet Schäden an der internen und / oder externen Reputation

Probleme in der Geschäftssteuerung:

Wichtige Daten und Informationen zur Steuerung des Unternehmens stehen nicht zur Verfügung (Kalkulationsdaten, Risikomanagement, Cash-, Liquiditäts- Bilanzdaten)

Verletzung gesetzl., regulatorischer Vorschriften:

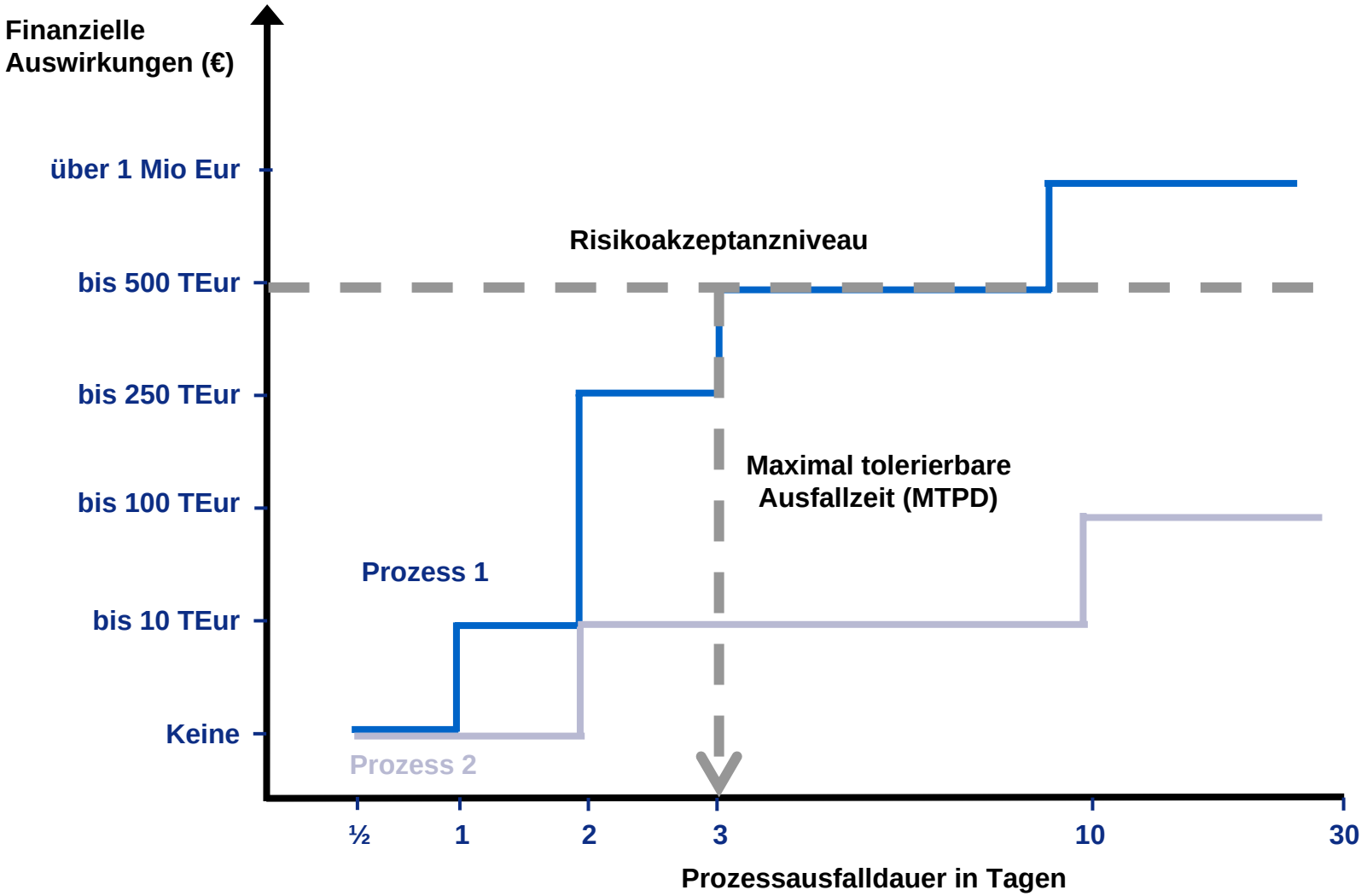
Gesetzliche oder regulatorische Anforderungen können nicht erfüllt werden



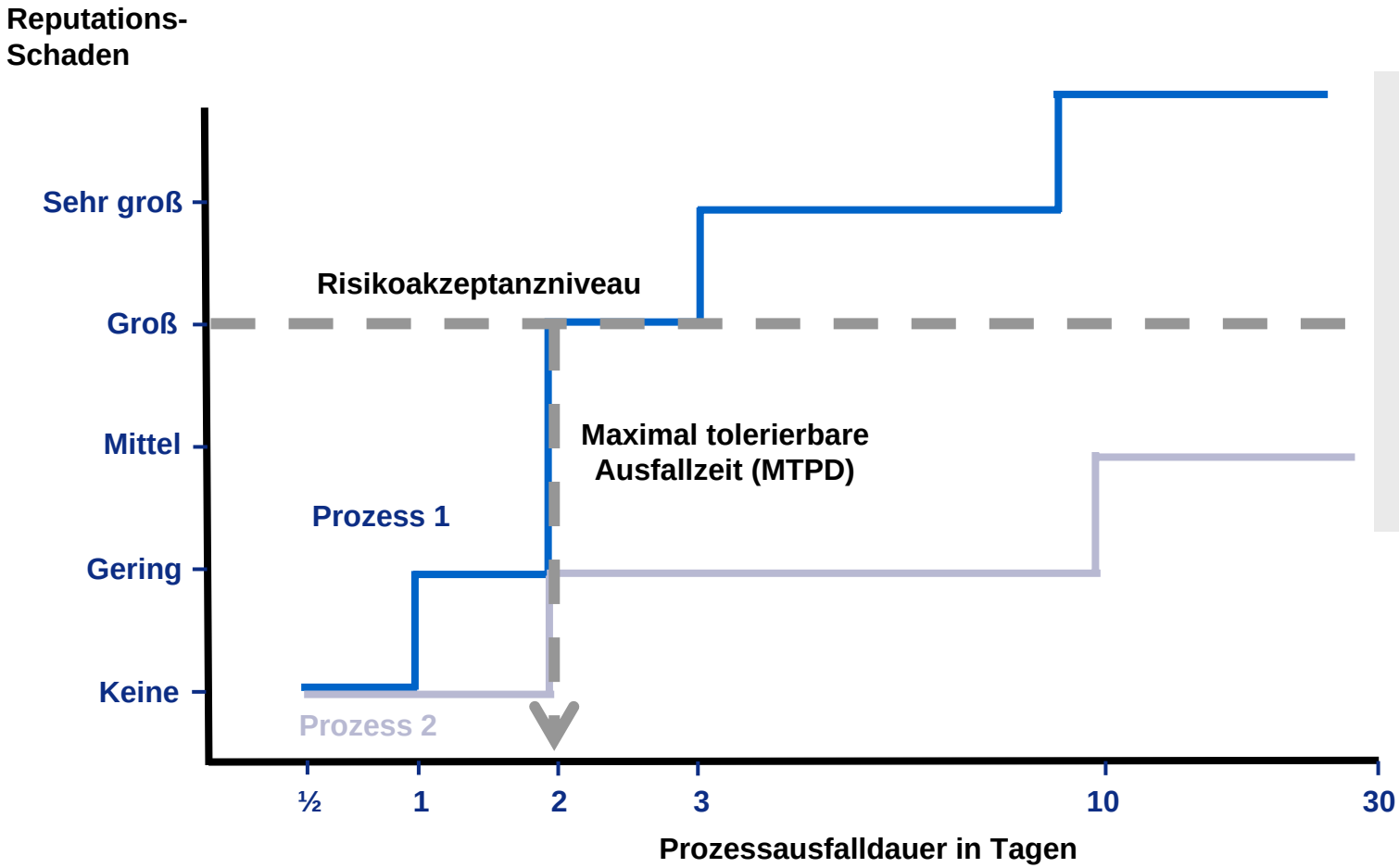
Definition der maximal tolerierbaren Ausfalldauer (Dringlichkeit)

Wie lange kann maximal auf die Durchführung des Prozesses verzichtet werden?

Die Ermittlung des finanziellen Impacts erfolgt in Schadensklassen über einen definierten Zeithorizont



Der Prozess erhält die minimale MTPD aus den Impact Kategorien



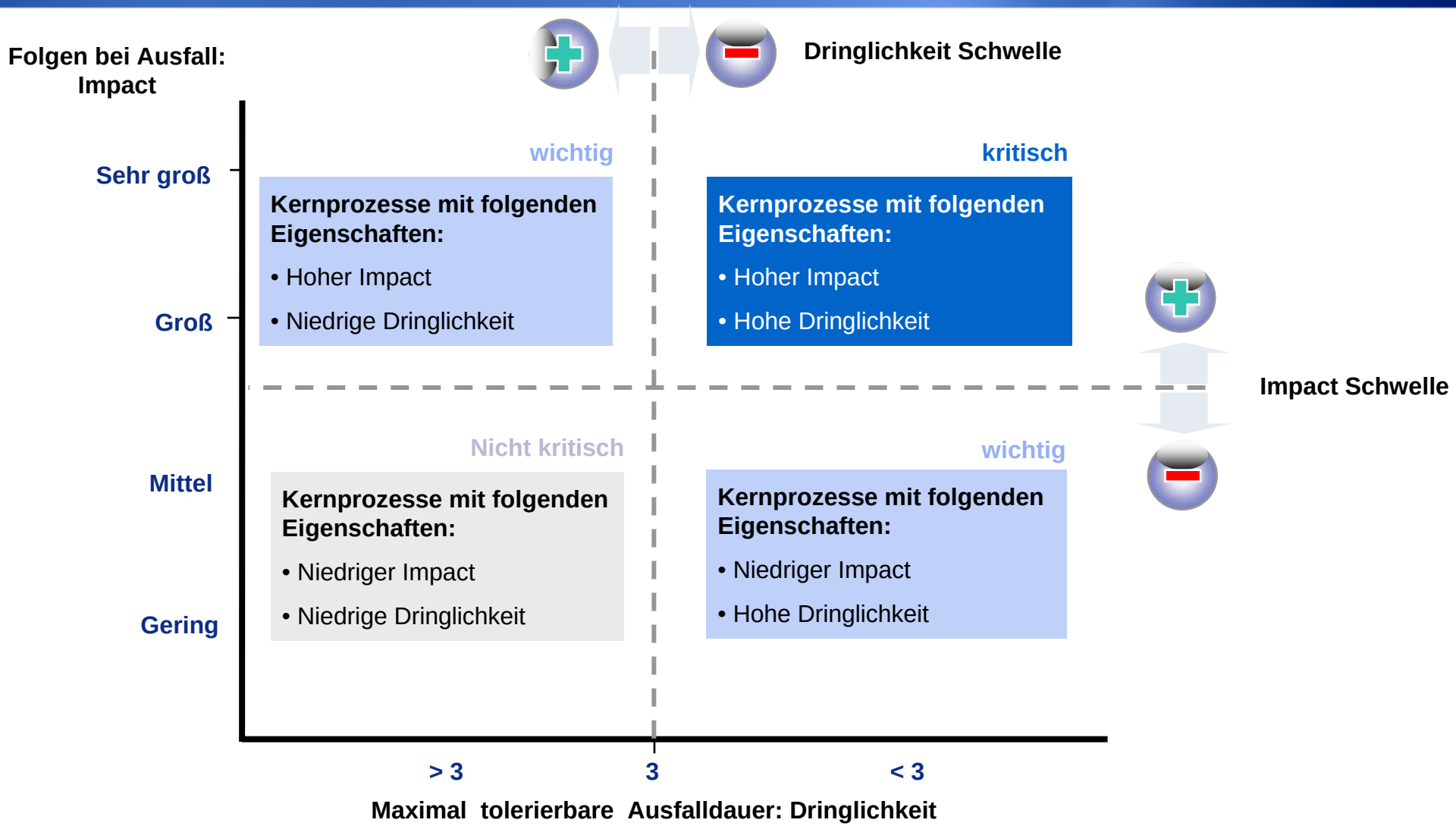
Gering:
Nur unternehmensinterne Beachtung

Mittel:
Reaktionen in der Presse (Lokal, Fachzeitungen)

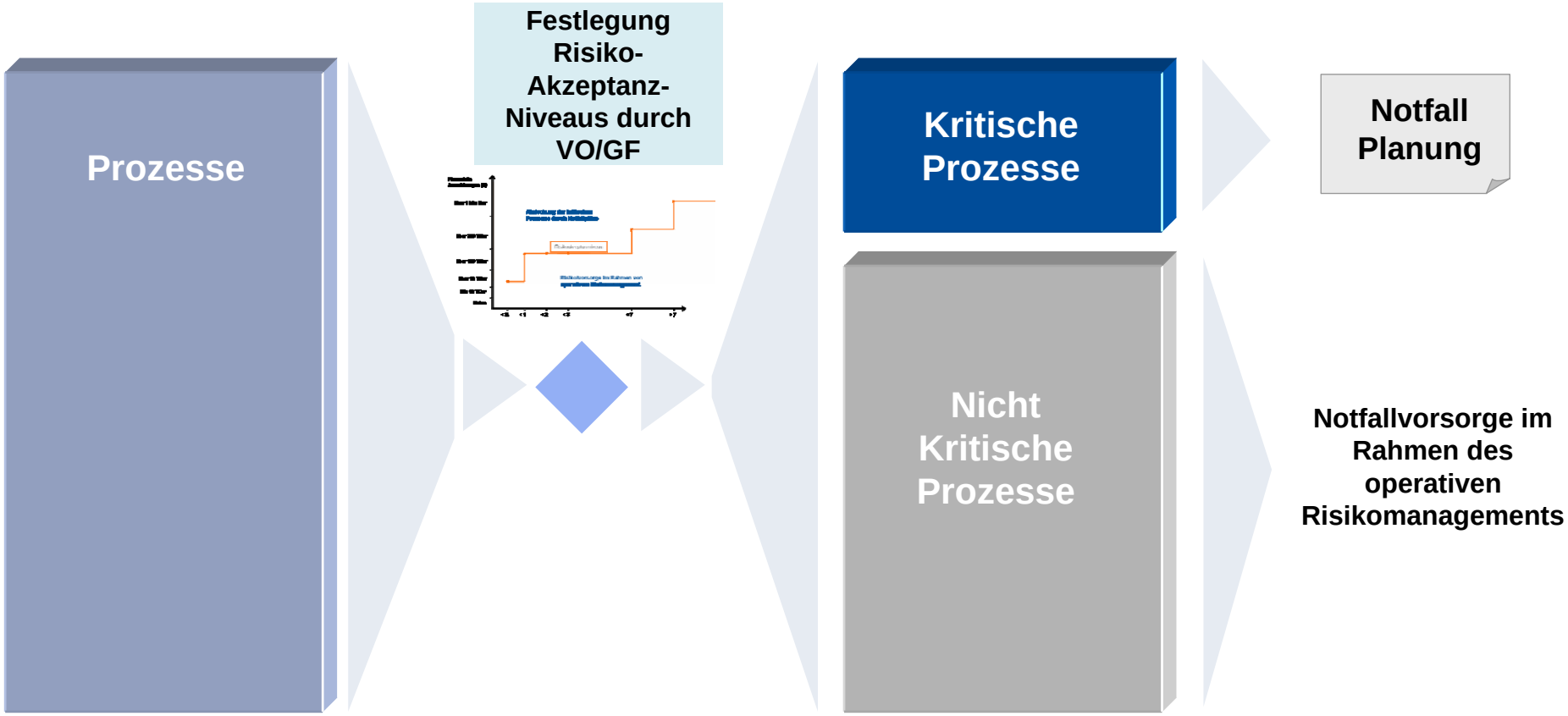
Groß:
Negative überregionale Medien und Presseveröffentlichungen, einzelne Kundenverluste

Sehr groß:
Negative Pressekampagne mit Kundenverlusten

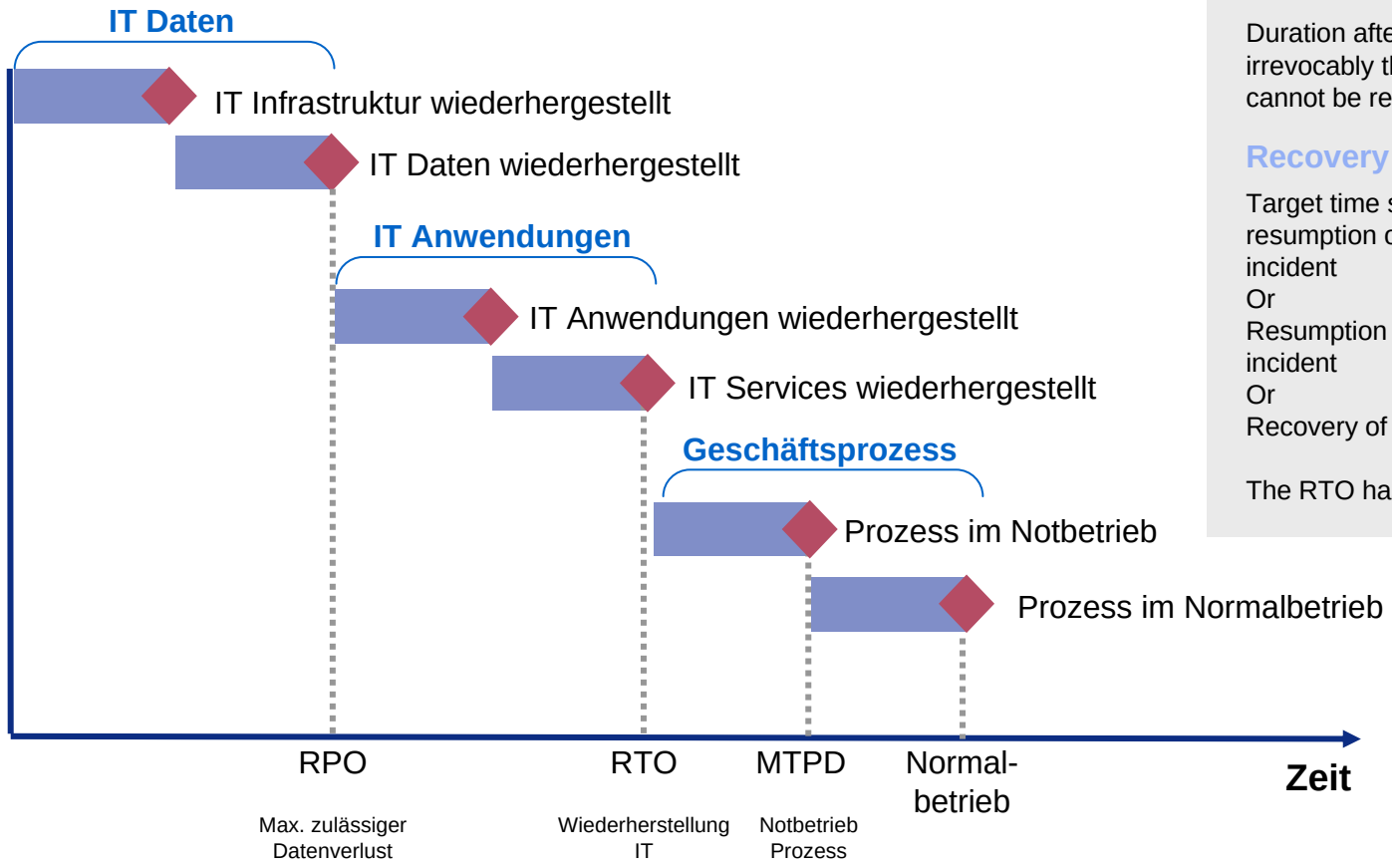
Durch die Festlegung des Risikoakzeptanzniveaus wird der Umfang der kritischen Prozesse gesteuert



Für die kritischen Geschäftsprozesse wird eine Notfallstrategie und Notfallplanung erarbeitet



MTPD und RTO werden oftmals nicht differenziert, Recovery Point Objective ist im Standard nicht definiert



Definitionen nach BS 25999

Maximum tolerable time of disruption (MTPD)

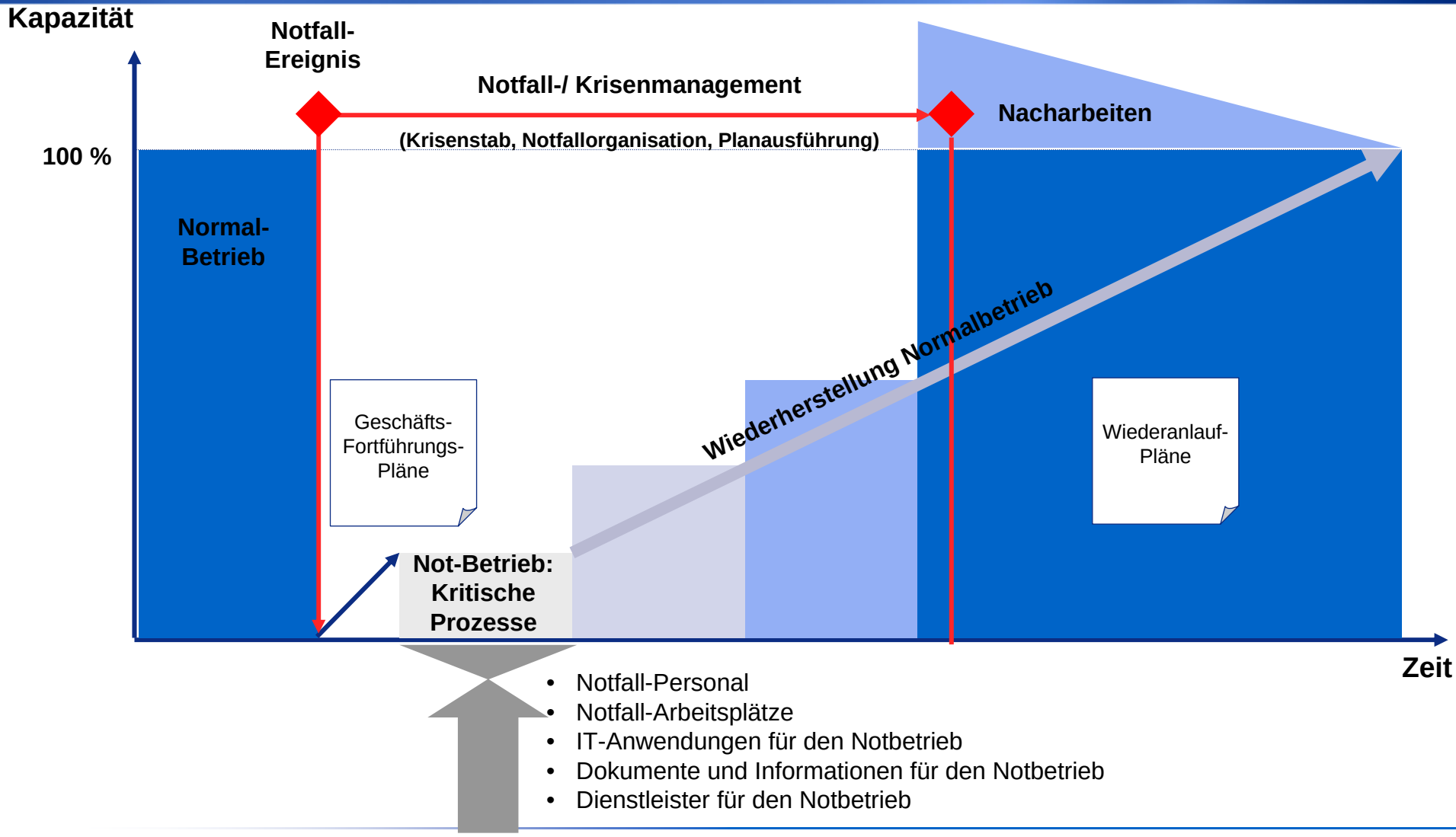
Duration after which an organization's viability will be irrevocably threatened if product and service delivery cannot be resumed

Recovery time objective (RTO)

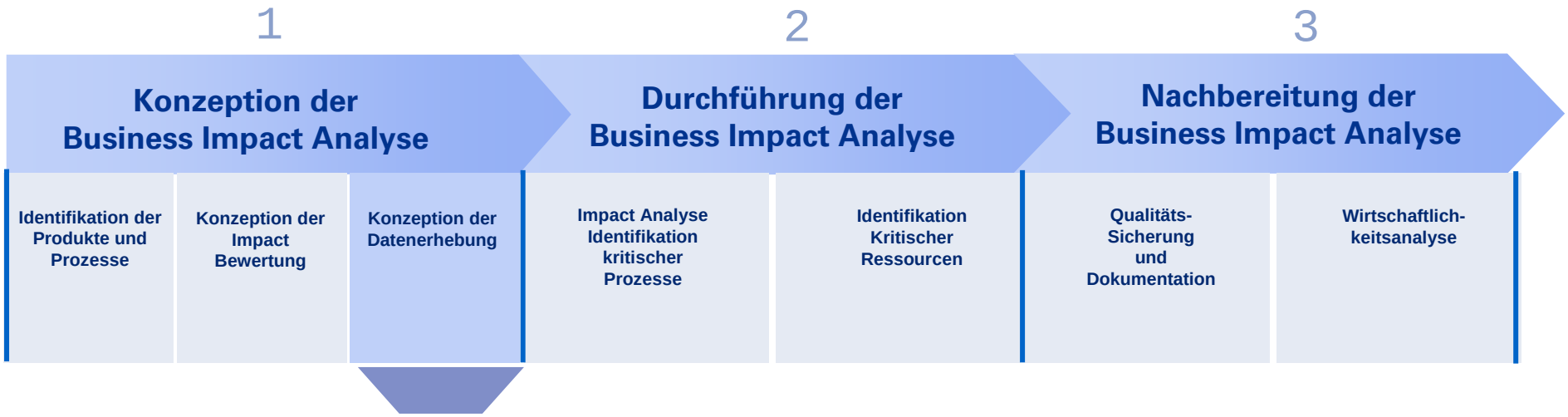
Target time set for
resumption of product, service or activity delivery after an incident
Or
Resumption of performance of an activity after an incident
Or
Recovery of an IT system or application after an incident

The RTO has to be less than MTPD

Die BIA beinhaltet die Beschreibung eines ersten Notbetriebs für die kritischen Prozesse



Die Form der Erhebung der BIA Daten bestimmt Aufwand aber auch Qualität der BIA Ergebnisse



Phase	Inhalt
Konzeption der Datenerhebung	• Festlegung der Vorgehensweise (Workshop, Interview, Questionnaire, Kombination) • Konzeption der Datenerhebung und Datenerfassung Ergebnisse: • Interviewleitfaden, Questionnaire, Workshop-Agenda • Projekt- und BCM-Präsentation • Werkzeuge zur Datenerfassung: BCM-Tool, Excel, Datenbank

Die Festlegung der Erhebungsform prägt die Awareness für das BCM

Festlegung der Vorgehensweise

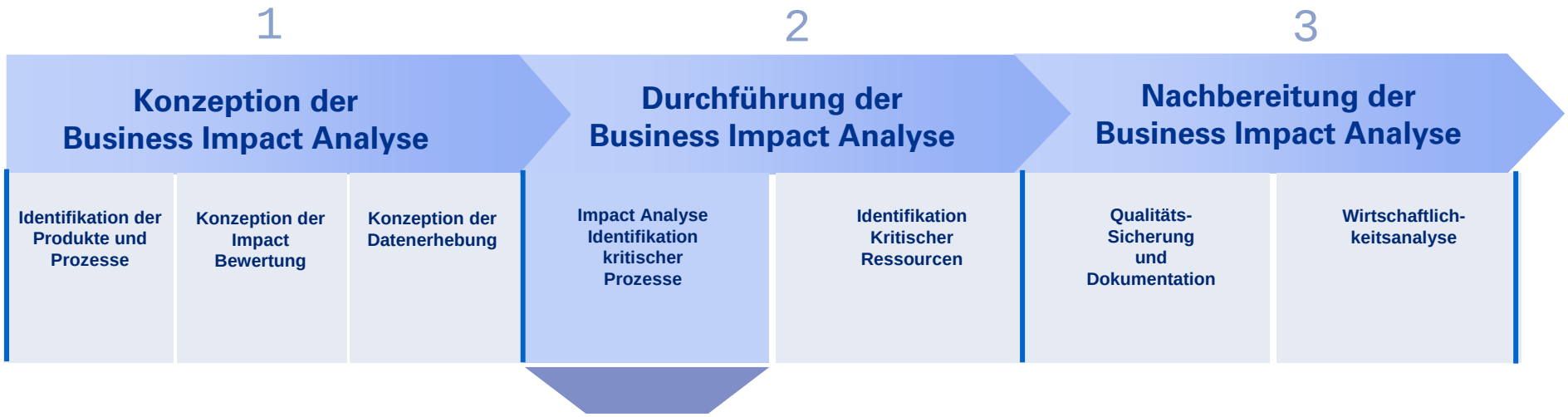
- Questionnaires
  - MS-Office-Templates oder BCM-Tool-basierte Questionnaires
  - Gefahr mangelhafter Datenqualität und schlechter Awareness bei ausschliesslich Questionnaire gestützter BIA!
- Workshops
  - Einführung in das Thema BCM und Awareness-Bildung
  - Erarbeitung der BIA im Workshop oder anschliessend dezentral
  - Wirtschaftliche Vorgehensweise, sorgfältige Vorbereitung erforderlich
- Interviews
  - Vor- und Nachbereitung der Datenerhebung in Einzelinterviews
  - Sehr aufwändig, aber sehr hohe Datenqualität und starke Awareness-Bildung
- Kombination
  - Kombination aus Workshops / Interviews und Questionnaire

Die Verwaltung der umfangreichen BIA-Daten sollte im Projekt frühzeitig konzipiert werden

Konzeption der Datenerhebung, -erfassung

- In einer BIA entstehen eine große Menge an Daten
  (Gemessene Datenmenge eines durchschnittlichen BIA Projektes: 32.000 zu pflegende Informationen!)
- Für die Daten ist ein Reporting notwendig
- Die Daten müssen regelmäßig überprüft und aktualisiert werden
- Die regelbasierte Vererbung von Kritikalitäten sprengt einfache Excel-Anwendungen
- Die Daten müssen revisionssicher abgelegt werden (Zugriffsschutz, Audit-Trail)
- Daher ist frühzeitig die Datenerfassung –und Speicherung zu klären
  - Eigenentwicklung auf Basis einer Datenbank
  - Einsatz eines BCM-Tools
  - Schnittstellen zu anderen Systemen bedenken: IT CMDB, Prozessmodellierungswerkzeug, HR-System etc.

Die Business Impact Analyse kann in zwei Teilschritte getrennt werden



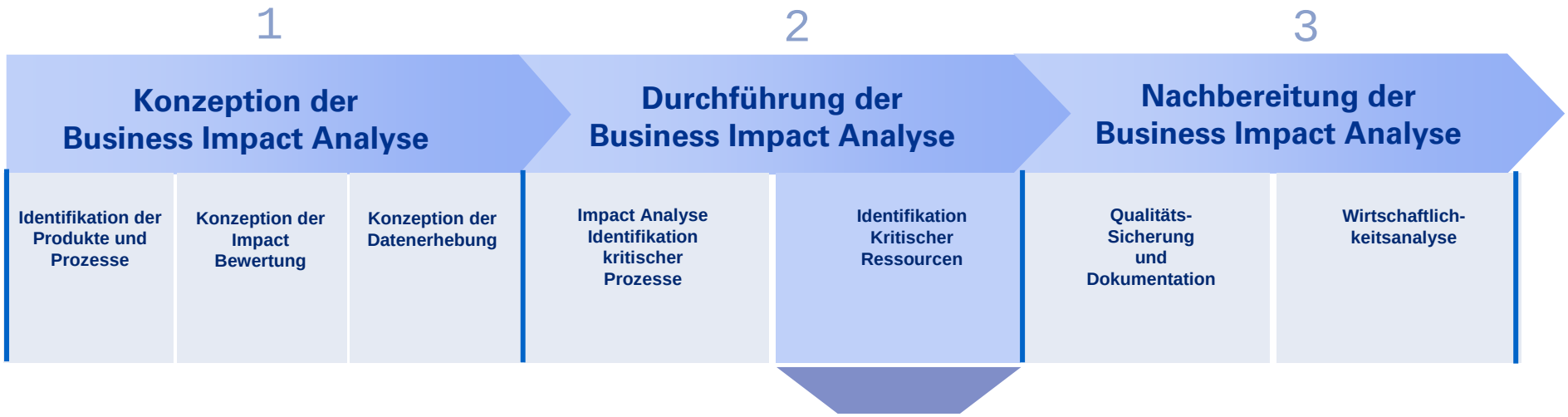
Phase	Inhalt
Identifikation kritischer Prozesse	• Vorstellung des Projekts zur Awareness-Bildung • Erhebung der Informationen im Rahmen der BIA auf Basis des Interviewleitfadens Ergebnisse: • Impact-Daten für die Geschäftsprozesse • RTO's

Die Impact Kategorien sind sorgfältig zu definieren um vergleichbare und nachvollziehbare Ergebnisse zu erzielen

Erhebung der Impact Daten:
Bsp. Interviewleitfaden

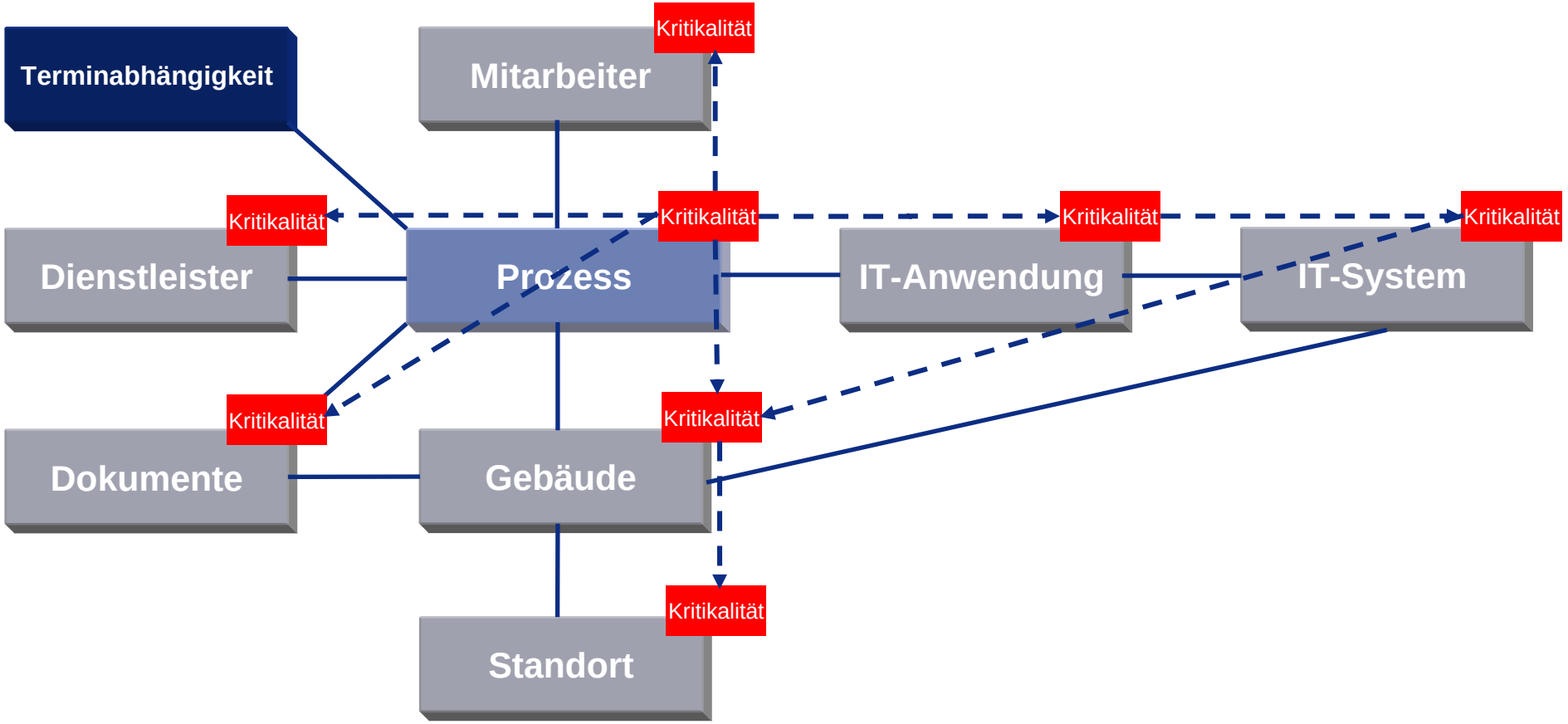
- Awareness für BCM schaffen
  - Projekt und BCM vorstellen mit Kurz-Präsentation
- Verständnis für das Geschäft entwickeln
  - Welches sind die Produkte, Dienstleistungen, Services?
  - Organisationsstruktur, Mitarbeiterstruktur
  - Informationen über die Märkte und Kunden
  - Mengengerüste und High / Low Seasons
  - Strategien für die Zukunft: Wachstumsfelder, Desinvestitionsstrategien
- Daten erheben
  - Geschäftsprozesse vollständig?
  - BIA-Daten erheben auf Basis des Questionnaires
- Weitere Vorgehensweise erläutern
  - Ausgefüllter Questionnaire zur Qualitätssicherung und Abnahme
  - Weiteres Projektvorgehen, nächste Schritte

Für die kritischen Prozesse werden in einer Detailerhebung die Ressourcen und deren Kritikalität ermittelt



Phase	Inhalt
Identifikation kritischer Ressourcen	• Identifikation der Ressourcen der kritischen Geschäftsprozesse • (regelbasierte) Vererbung der Kritikalität von den Geschäftsprozessen auf die Ressourcen • Mengen und kritische Termine der Geschäftsprozesse Ergebnisse: • Zuordnung der Ressourcen zu den Geschäftsprozessen • Kritikalität der Ressourcen (RTO über Vererbung)

Die Kritikalität (RTO) wird regelbasiert auf die Prozess-Ressourcen vererbt



Die Ressourcen erben die Kritikalität mehrer Prozesse, Regeln leiten hieraus die Kritikalität der Ressource ab (Bsp. minRTO)

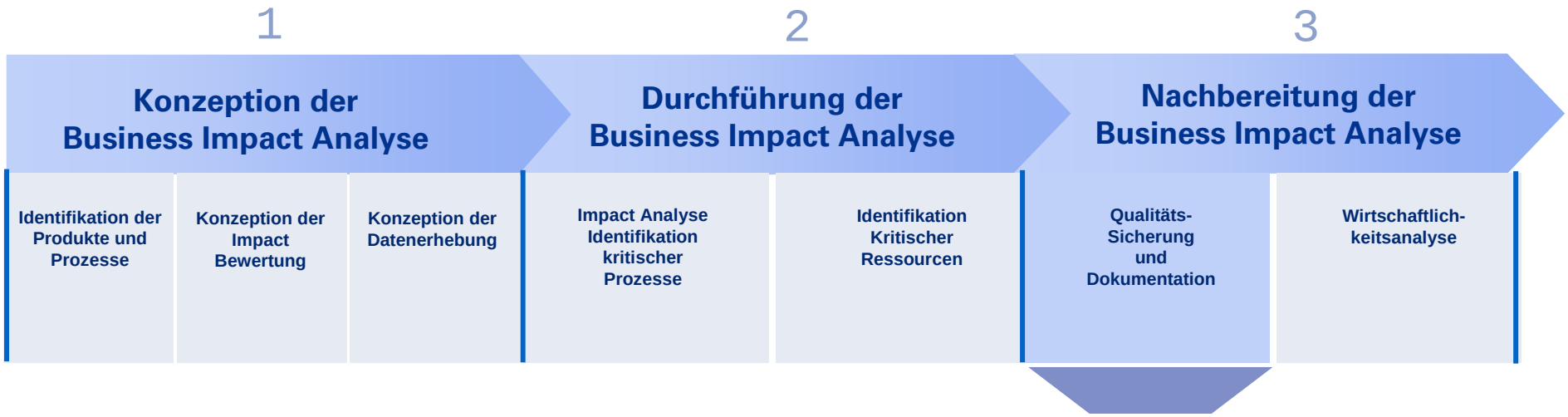
Erhebung der Ressourcen

- Die Erhebung der Prozess-Ressourcen sollte gut vorbereitet werden, um konsistente Daten zu erhalten
  - Liste der IT-Anwendungen (eindeutige Benennung!)
  - Liste wichtiger interner und externer Dienstleister
  - Liste zentraler Dokumente
- Wird die Ressource im Notbetrieb benötigt?
- Werden an die Ressource im Notbetrieb andere Anforderungen als im Normalbetrieb gestellt (Mengen, Zugriff von anderem Standort etc.)?
- Wer ist für die Ressource verantwortlich (Service Level Management, Verträge)?

Vererbung der Kritikalität

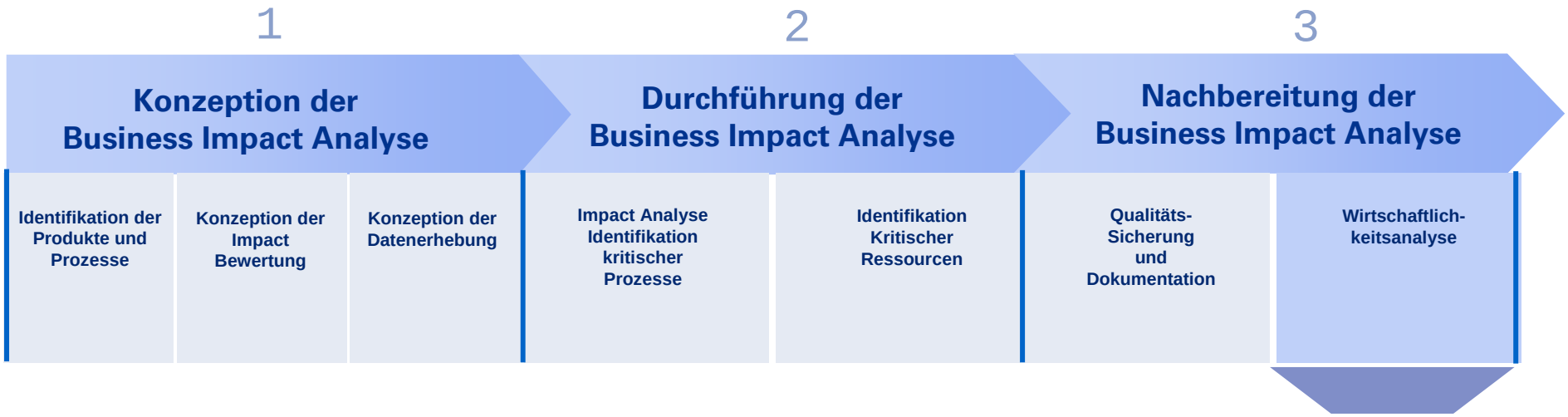
- Für die Vererbung der Kritikalität sind Regeln zu definieren. Beispiel: die geringste MTPD wird auf den Prozess vererbt

Die erhobenen BIA-Daten sind auf unternehmensweite Konsistenz zu sichern und die Anforderungen zusammenzustellen



Phase	Inhalt
Qualitätssicherung und Dokumentation der BIA	• Konsistenz der erhobenen Daten sichern • Auswertungen und Reporting über die BIA-Ergebnisse für das Management • Festlegung der Risikoakzeptanzniveaus durch das Top-Management (ex post) Ergebnisse: • Qualitätsgesicherte BIA-Daten • Reports für Management und IT über die erhobenen Anforderungen (MTPD, RTO, RPO, Notbetriebsanforderungen) • Grundlagen für Strategieentwicklung und Notfallplanung

Die Wirtschaftlichkeit der Anforderungen aus der BIA muß sichergestellt sein, gegebenenfalls Anforderungen reduziert werden



Phase	Inhalt
Wirtschaftlichkeits-Analyse	• Grobe Kostenabschätzung für die Umsetzung der Anforderungen (insbesondere IT und Facility Management) • Balancierung von Anforderungen und Kosten Ergebnisse: • Abgestimmte Anforderungen an Wiederanlauffristen und Notbetriebsanforderungen • Abgestimmter Input für Notfallstrategie und Notfallplanung • Abgestimmter Input für IT Service Continuity Management

Quellen

bci Good Practice Guidelines 2008 Section 2: Understanding the organisation	The Business Continuity Institute www.thebci.org Englisch, kostenfrei Deutsche Fassung: GPG 2005
BS 25999-1:2006 Code of Practice	British Standard http://www.bsi-global.com/en/Standards-and-Publications/Industry-Sectors/Risk/Business-continuity/ Kostenpflichtig
BS 25999-2:2007 Specification	British Standard http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030169700 Kostenpflichtig
BSI 100-4 Notfallmanagement Entwurf Version 0.7	Bundesamt für Sicherheit in der Informationstechnik http://www.bsi.de/literat/bsi_standard/index.htm Kostenfrei

AGENDA

Inhalt

- **Die Business Impact Analyse im BCI GPG und BS 25999**
- **Best Practices und Stolperfallen**
- **Diskussion**

Vielen Dank für Ihre Aufmerksamkeit

Fragen ? / Diskussion

Matthias Hämmerle MBCI

Senior Manager
KPMG DTAG
Marie-Curie-Strasse 30
60439 Frankfurt / Main
49 (69) 9587-4960
49 (173) 5764211
mhaemmerle@kpmg.com