Advisory

Die Schnittstellen zwischen BCM und ITSCM

Business Continuity Management
Gesellschaft für Informatik e.V.
26.06.2009

Matthias Hämmerle MBCI

AGENDA

Inhalt

- **Standards für BCM und ITSCM**
- **BS 25999 und BS 25777 im Zusammenspiel**
- **Schnittstellen BCM und ITSCM entlang des BS 25777 Lifecycle**

IT SCM Management - Steuerung und Regelung

IT Service: Beschreibung einer IT-Dienstleistung aus Sicht des Kunden, welche die Geschäftsprozesse unterstützt

Verfügbarkeit: Die Wahrscheinlichkeit oder das Maß, dass ein technisches System bestimmte Anforderungen zu bzw. innerhalb eines vereinbarten Zeitrahmens erfüllen muss

IT SCM ist das Management der optimalen Verfügbarkeit von IT Services mit dem Ziel der Sicherstellung der Verfügbarkeit, unter Berücksichtigung der Wirtschaftlichkeit.

Nicht die technischen Wünsche und Machbarkeiten, sondern die Geschäftsanforderungen sind für das IT SCM maßgeblich

IT SCM ist ein Management-Prozess, der einen strategischen und operationellen Rahmen bereitstellt, um

- Klare Rollen und Verantwortlichkeiten für IT SCM festzulegen
- Klare Schnittstellen zu anderen Prozessen zu gewährleisten
- Methoden zur Messung, Reportingstruktur und Kontrollsystem zu implementieren
- Regelmäßige Tests, angemessene Wartung und Audits durchführen
- Die IT SCM Policy zu definieren unter Berücksichtigung und Einbindung der regulatorischen Anforderungen, Standards und Rahmenbedingungen

IT Service Continuity Management weist zahlreiche Schnittstellen zu IT- und Fachbereichsprozessen auf

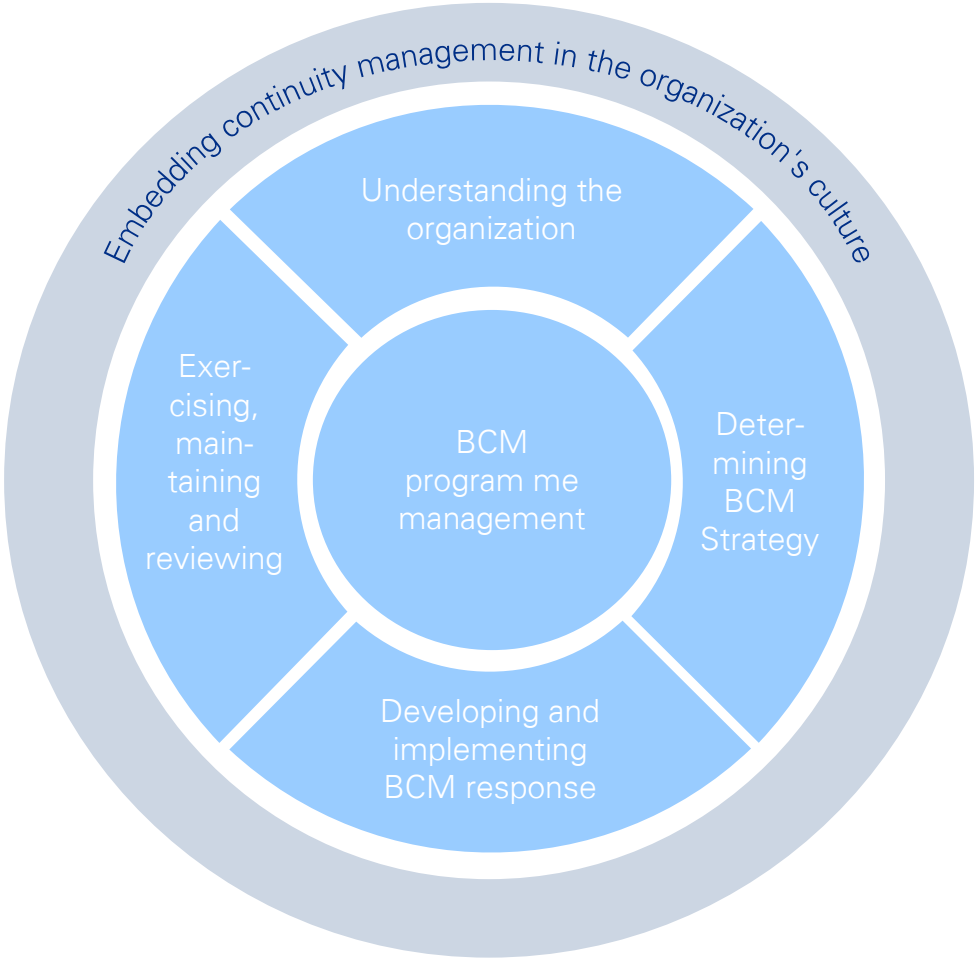
Nationale und internationale Normen für BCM und ITSCM

AGENDA

Inhalt

- **Standards für BCM und ITSCM**
- **BS 25999 und BS 25777 im Zusammenspiel**
- **Schnittstellen BCM und ITSCM entlang des BS 25777 Lifecycle**

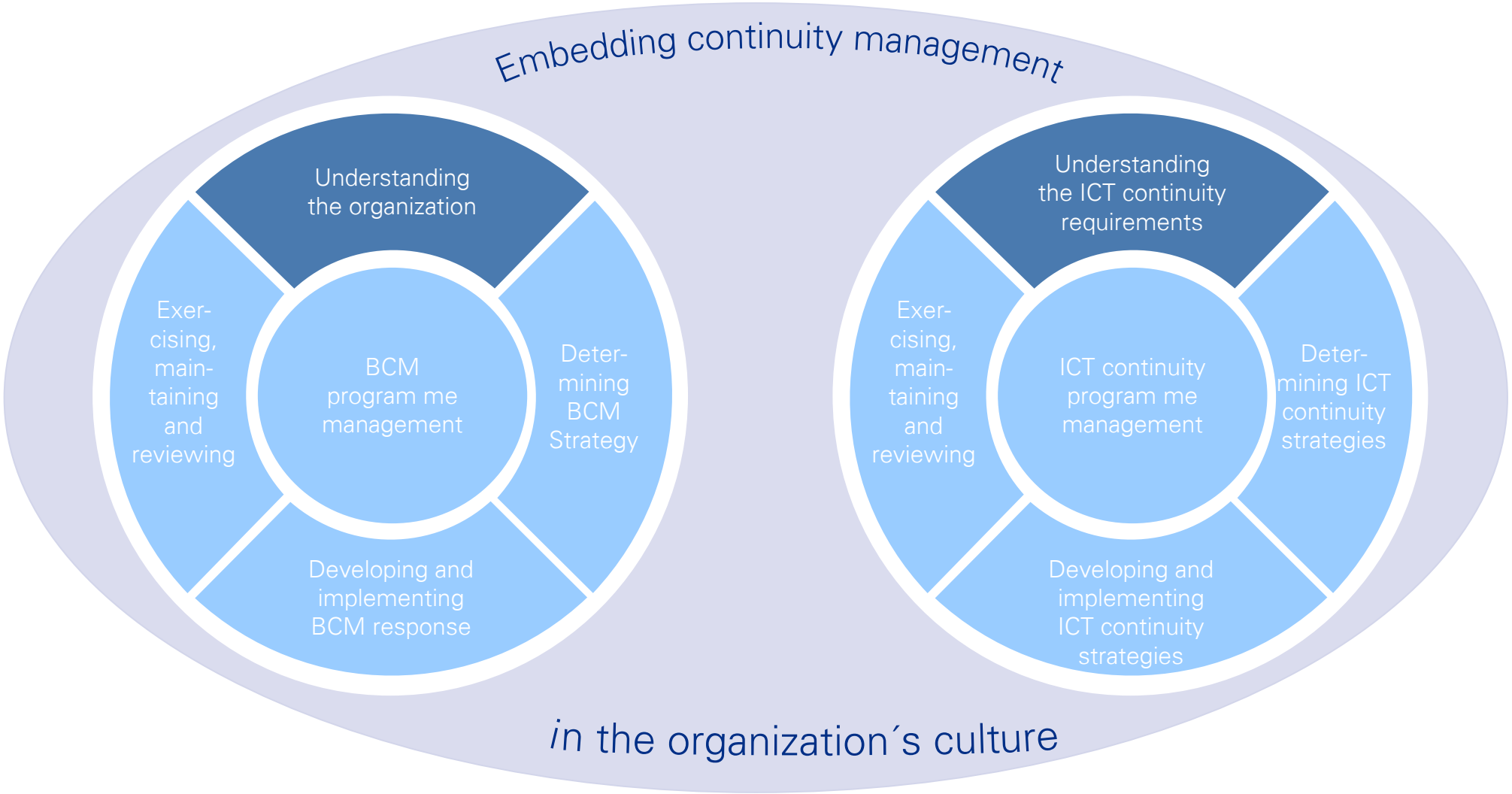
Der Lifecycle für das Business Continuity Management nach BS 25999-1



Der (BCM-Lifecycle gliedert sich in 6 Dimensionen:

1. BCM-Programm Management
   - Schaffung eines unternehmensweiten BCM-Zielbildes
2. Verständnis des Geschäftsmodells
   - Ermittlung der kritischen Geschäftsprozesse m (BIA)
   - Risikoanalyse (RIA)
3. Entwicklung von Kontinuitätsstrategien
   - Festlegung der strategischen Optionen
   - Schaffung eines Gleichgewichtes zwischen Investition und Risikobereitschaft für die Geschäftsfortführung der identifizierten geschäftskritischen Prozesse
4. Entwicklung und Implementierung von BCM – Plänen und Lösungen
   - Konkrete Ausfallplanung für die einzelnen Ressourcen und Gefährdungsszenarien
5. Übung, Anpassung und Audit
   - Übungs- und Testzyklen,
   - Anpassung des BCM-Zielbildes, Self-Assessments gegenüber dem BCM Zielbild
   - Internes und externes Audit des BCM
6. Aufbau und Verankerung einer BCM – Kultur
   - Integration des BCM in die Unternehmenskultur,
   - Schaffung von Motivation und Verantwortungsbewusstsein der Mitarbeiter

BS 25999 und BS 25777 ergänzen sich im methodischen Vorgehensmodell



AGENDA

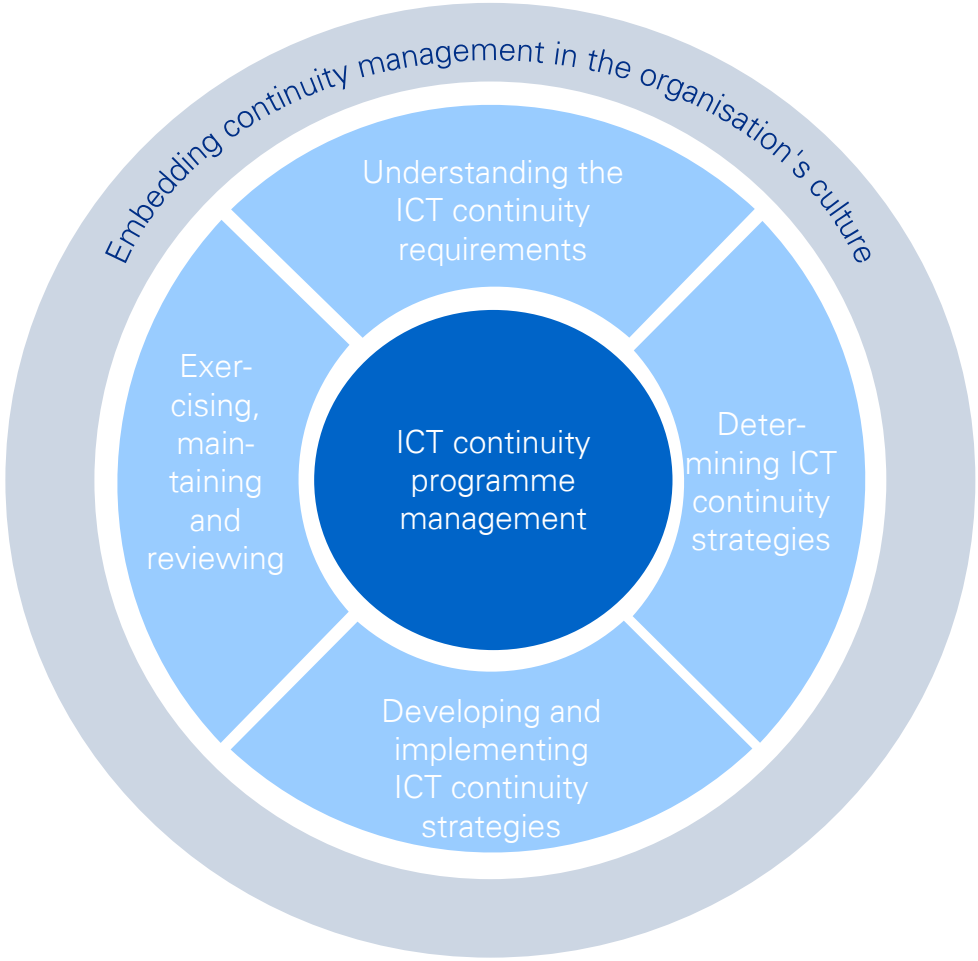
Inhalt

- **Standards für BCM und ITSCM**
- **BS 25999 und BS 25777 im Zusammenspiel**
- **Schnittstellen BCM und ITSCM entlang des BS 25777 Lifecycle**

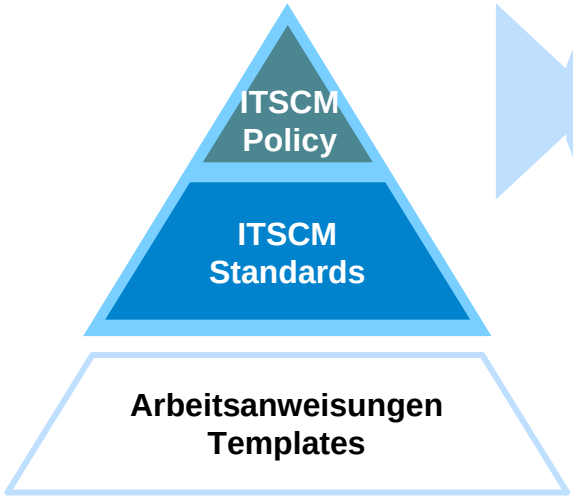
BS 25777-Lifecycle: Programm-Management

ICT Programm Management

- Implementierung eines Management Systems für das ICT Continuity Management
- Festlegung von Zielen und Umfang (Scope)
- ICT Continuiy Policy
- Bereitstellung der Ressourcen

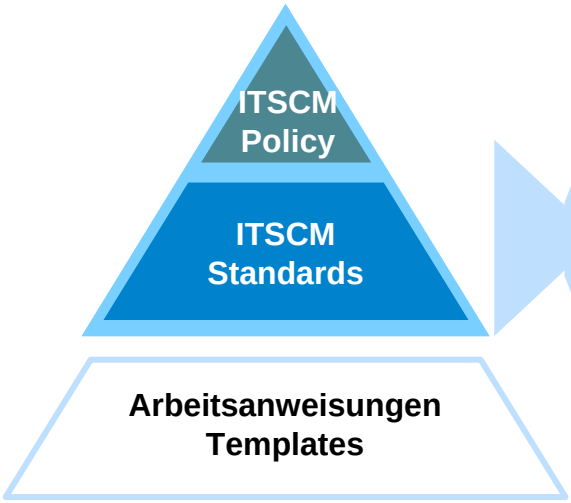


Die ITSCM Policy formuliert das Leitbild des ITSCM und die Rahmenbedingungen für die Implementierung und den Betrieb



- **Inhalte der ITSCM – Policy**
  - Ziele und Leitgedanke des ITSCM
  - Verantwortlichkeit des Vorstands / der Geschäftsführung
  - Definition und Ziele
  - Abgrenzung des Umfangs
  - Rechtliche und regulatorische Anforderungen und Normen
  - Umsetzung des ITSCM
    - Methoden, Verfahren, Standards
    - Organisation
    - Schnittstellen

ITSCM Standards beschreiben die konkrete Vorgehensweise sowie die Organisation / Rollen

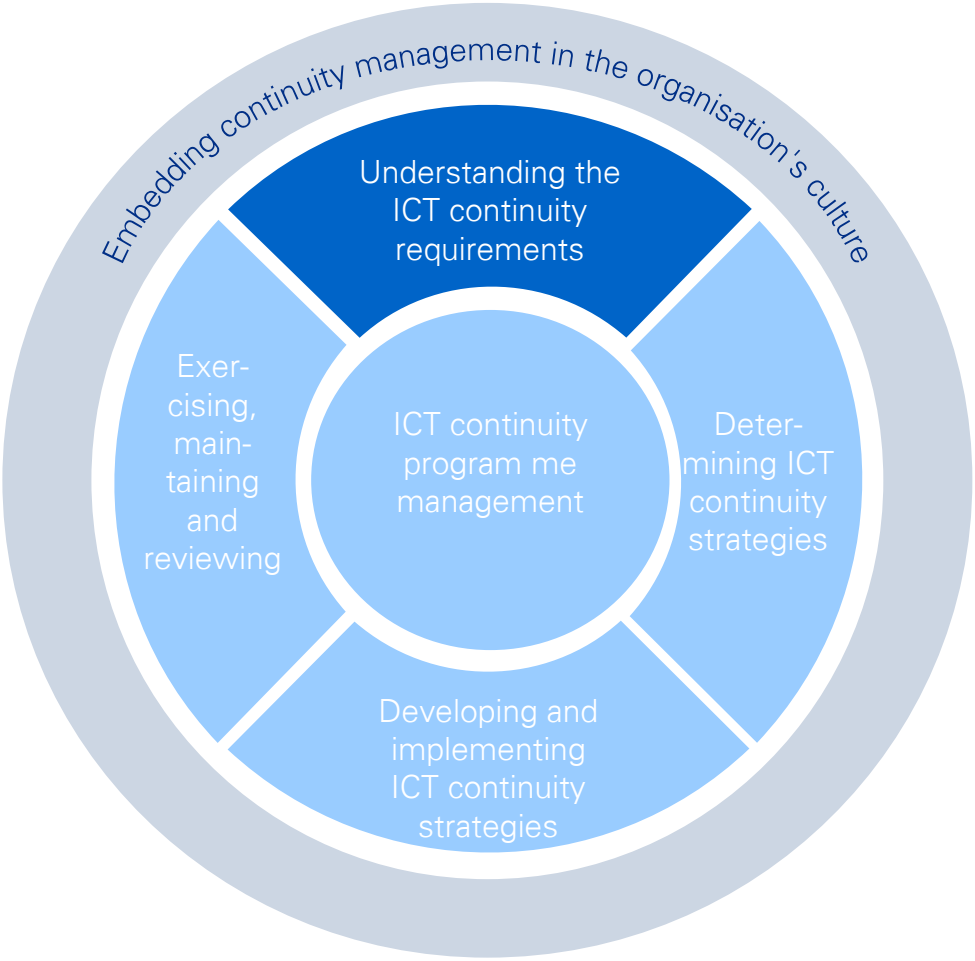


- **Inhalte des ITSCM – Standards**
  - Begriffsdefinitionen, Glossar
  - Rollen und Verantwortlichkeiten, AKV
  - ITSCM Prozess Beschreibung
  - Schnittstellen zu anderen IT Prozessen (ITIL-Prozesse)
  - Schnittstellen zum BCM

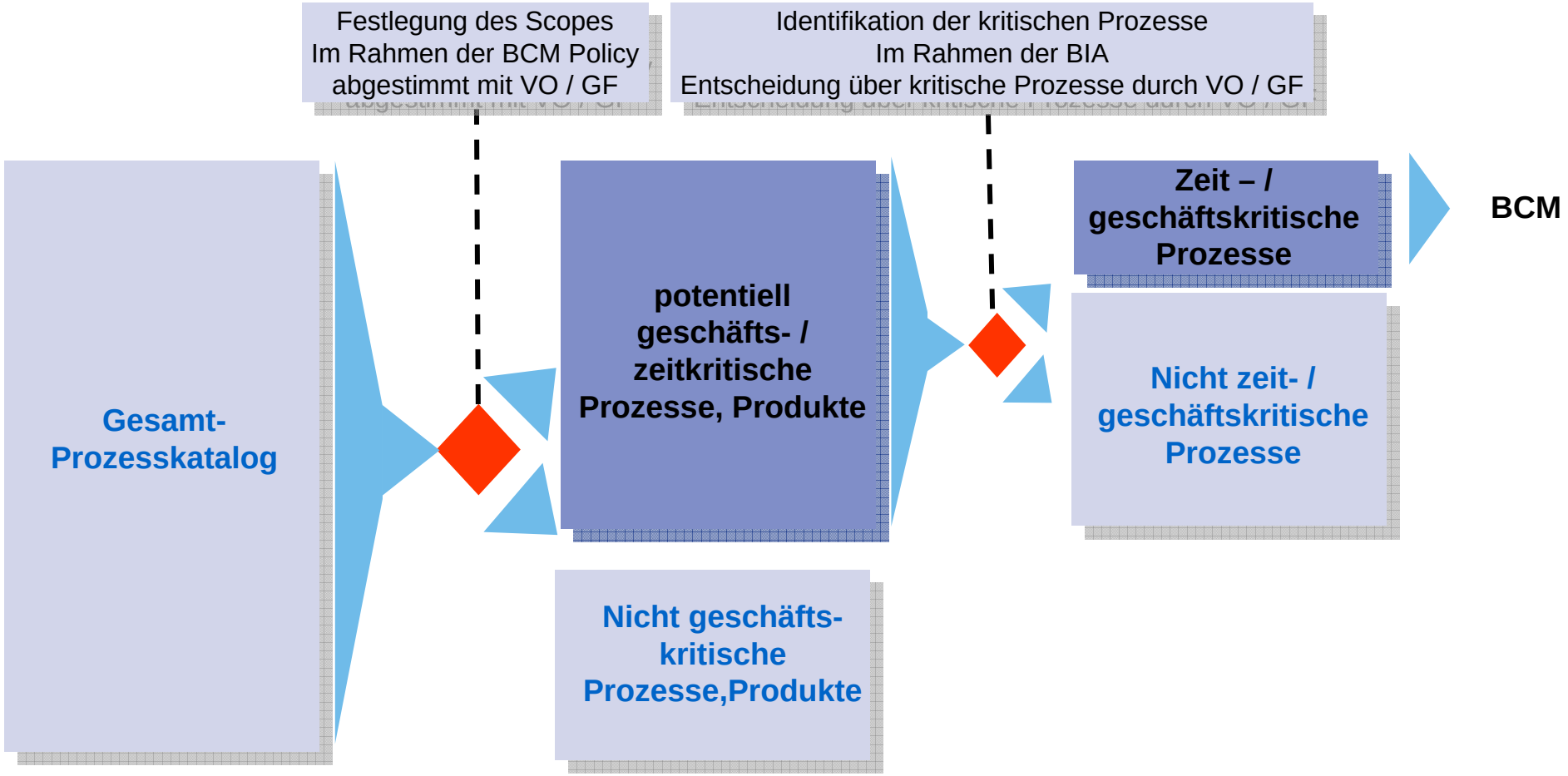
BS 25777-Lifecycle: Verständnis der Anforderungen

Verständnis der Anforderungen an das ICT Continuity Management für das Business Continuity Management

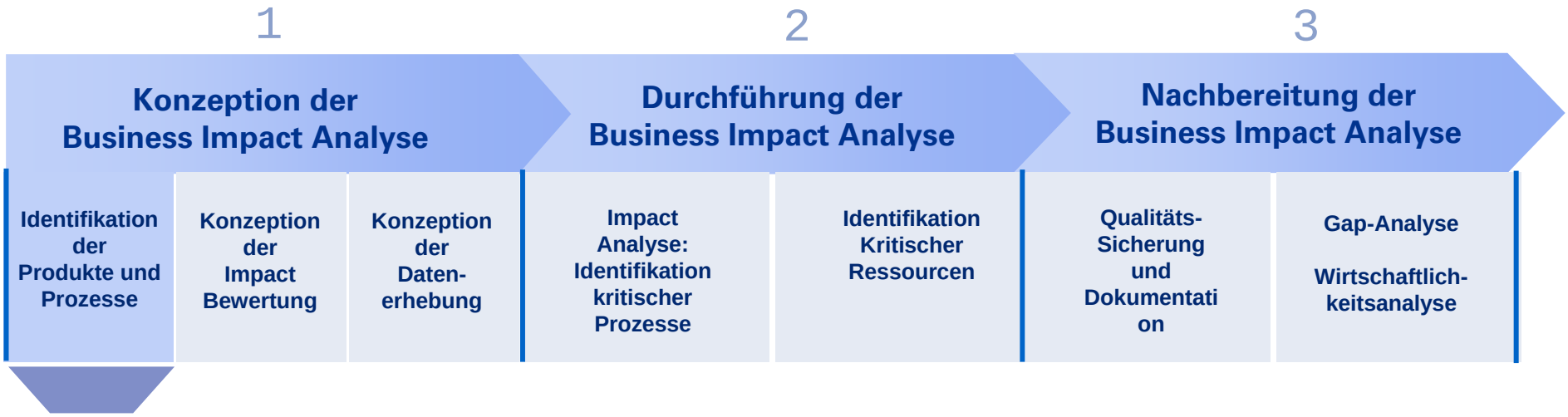
- Festlegung der Anforderungen an das ICT Continuity Management zur Erfüllung der Anforderungen des Business Continuity Managements
  - (zeit-) kritische Prozesse
  - RTO´s für kritische Prozesse
  - kritische Termine
  - Notbetriebsanforderungen
- Mapping auf die IT-Services
  - Definition der IT-Services
  - Identifikation der für das BCM relevanten IT-Services
  - Festlegung der kritischen IT-Services
- Identifikation der Komponenten, die für die kritischen IT-Services erforderlich sind
- Gap-Analyse



In zwei Schritten werden die geschäftskritischen Prozesse identifiziert

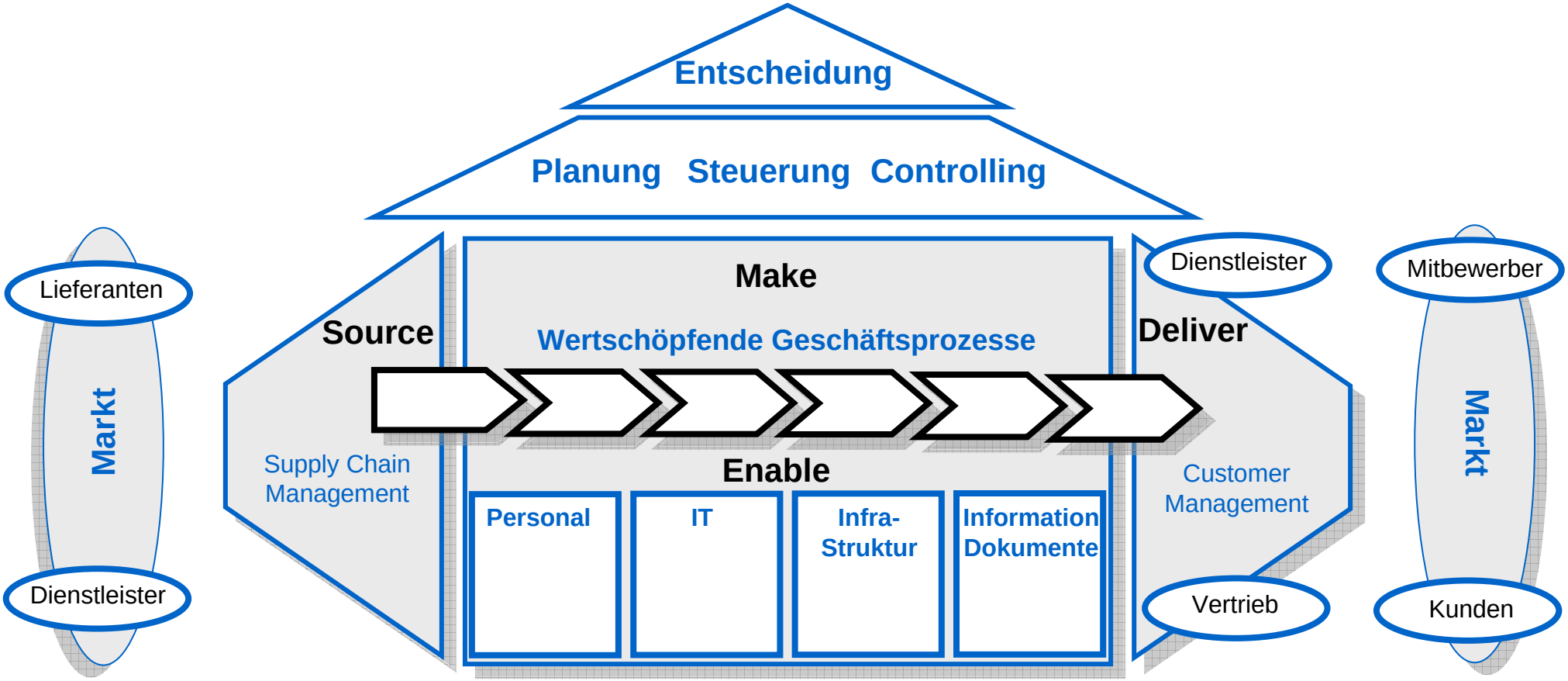


Zentraler Schritt ist die Festlegung des Scopes des BCM

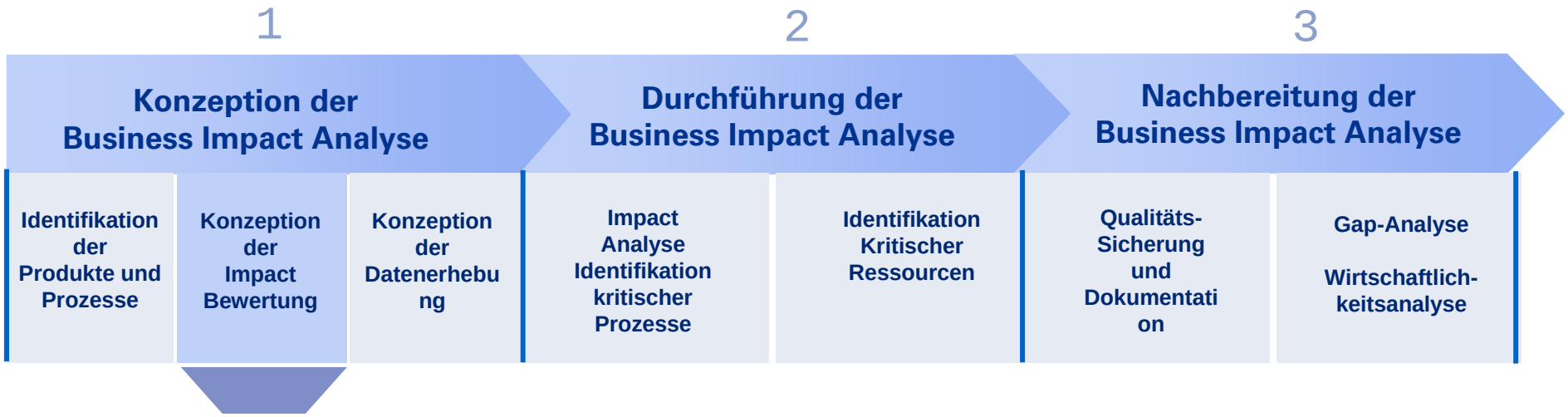


Phase	Inhalt
Identifikation der relevanten Produkte und Prozesse	• Abgrenzung der relevanten Organisationsbereiche • Sammlung und Auswertung vorhandener Prozessdaten Ergebnisse: • Definierter und freigegebener Scope für die BIA • Prozesskatalog als Grundlage für die BIA

Das BCM muß die Verfügbarkeit der kritischen Wertschöpfungsketten sicherstellen



Das Impact-Bewertungsmodell ist das methodische Kernelement der BIA



Phase	Inhalt
Konzeption der Impact Bewertung	• Festlegung der Impact Kategorien (Bsp.: 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

Ziel der Business Impact Analyse ist eine Klassifizierung der Prozesse nach ihrer Kritikalität

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:

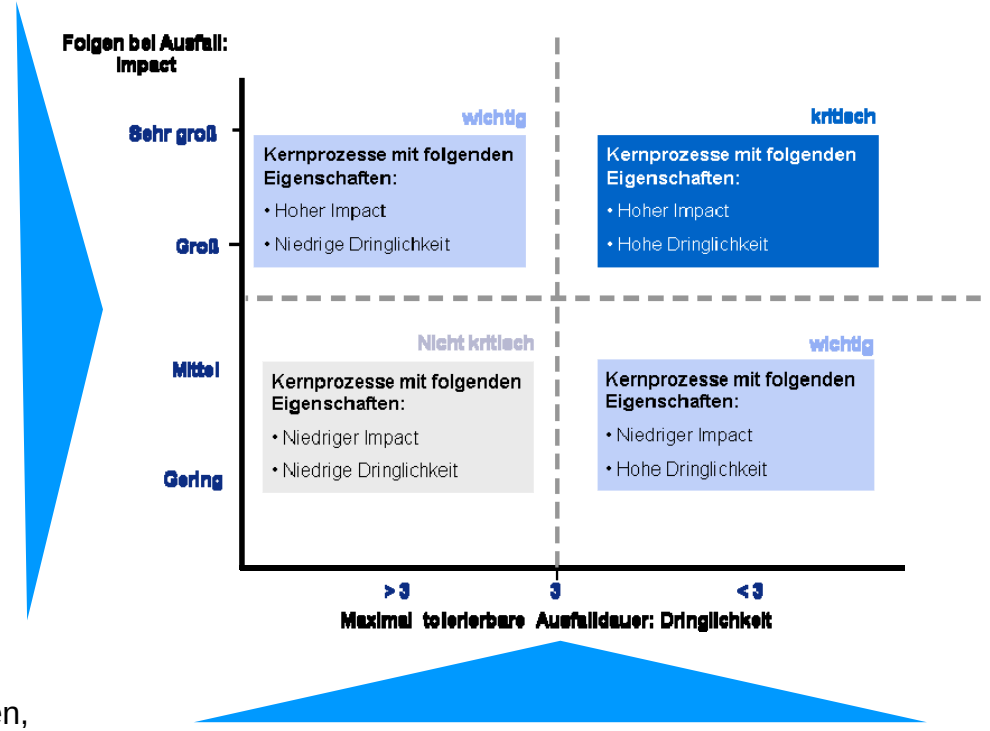
Das Unternehmen erleidet Schäden an der internen und / oder externen Reputation

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:

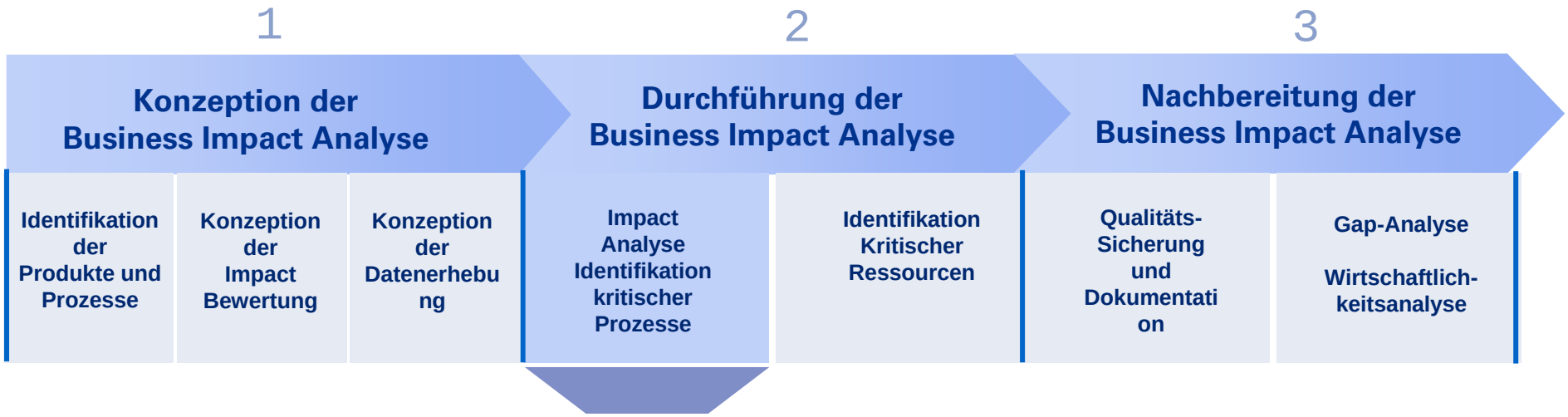
Gesetzliche oder regulatorische Anforderungen können nicht erfüllt werden



Definition der maximal tolerierbaren Ausfalldauer (Dringlichkeit)

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

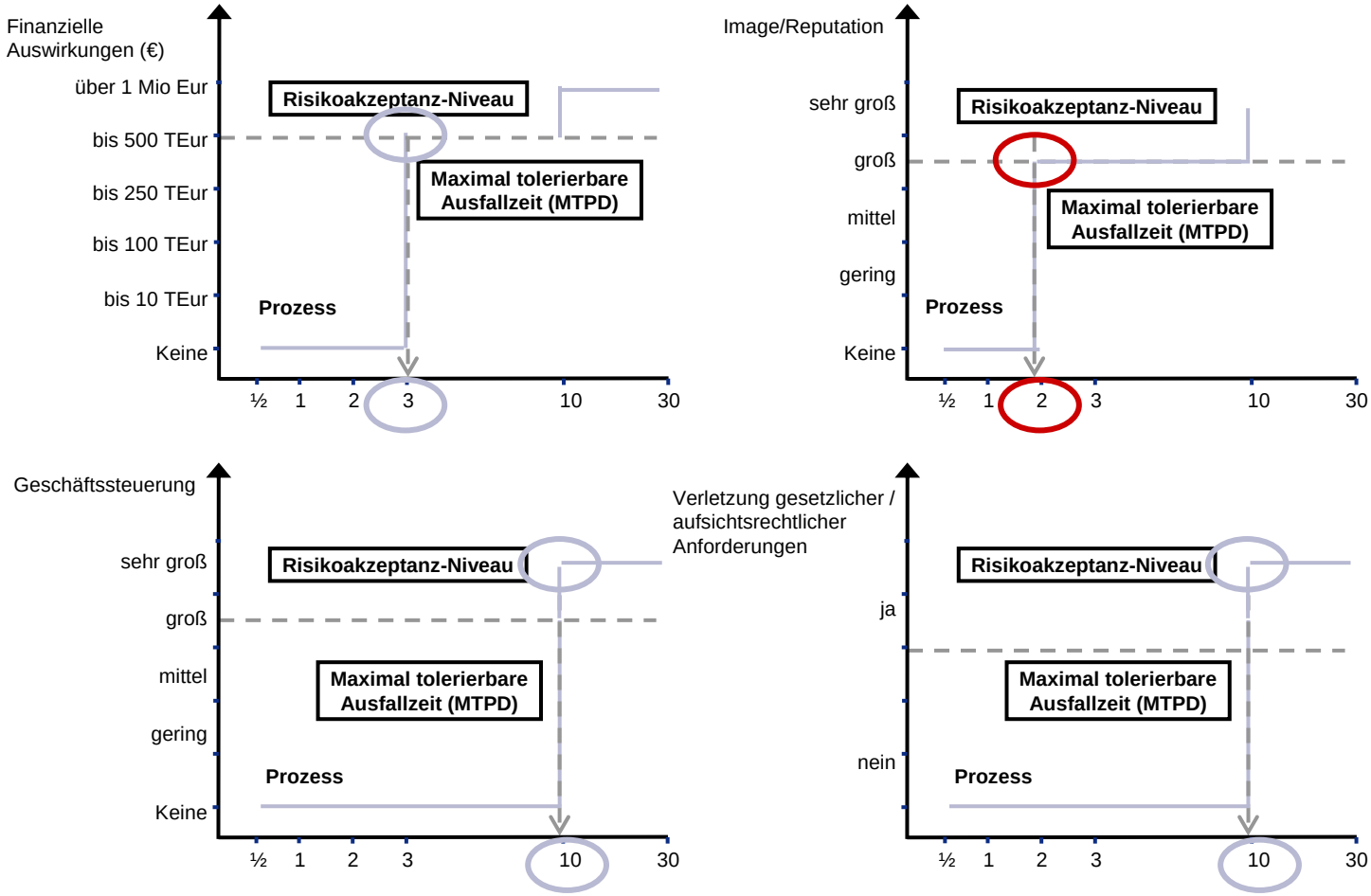
Die Business Impact Analyse kann in zwei Teilschritte getrennt werden



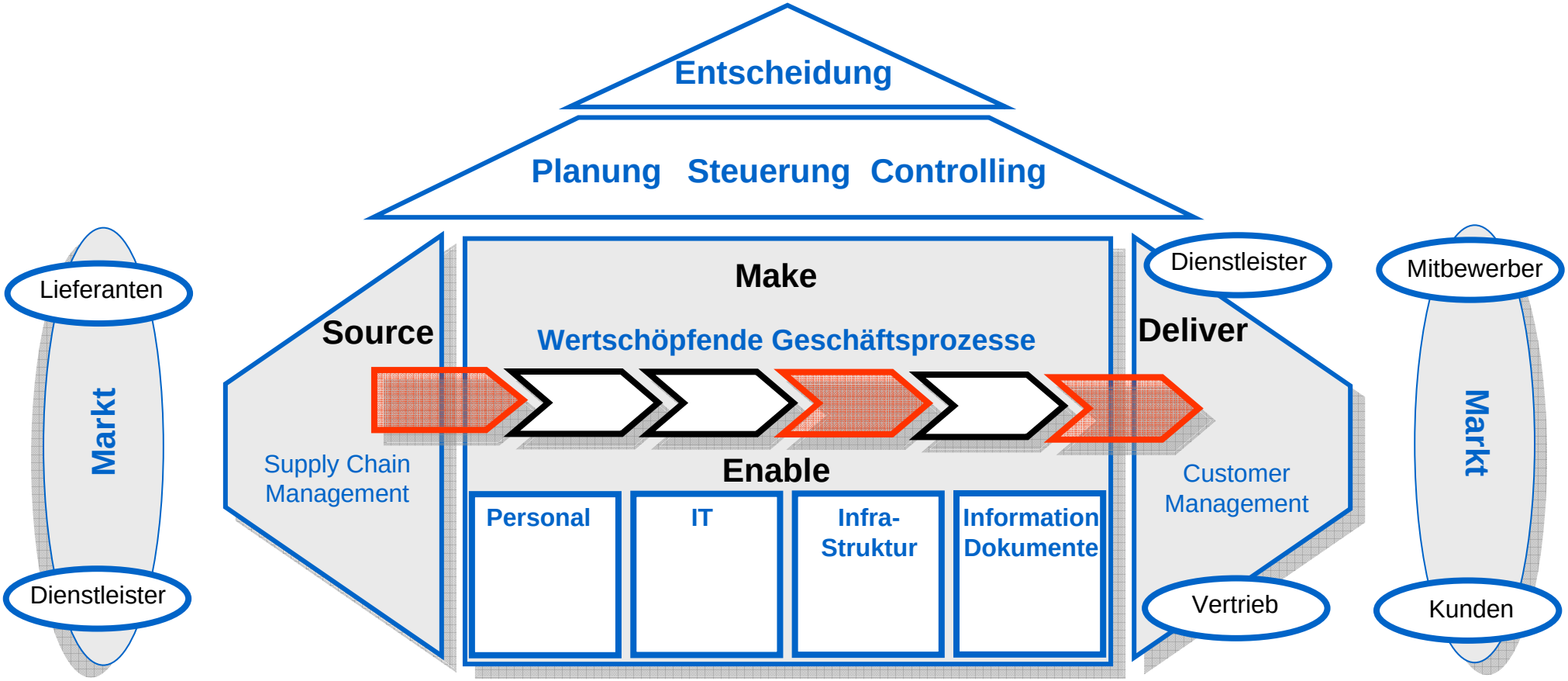
Phase	Inhalt
Identifikation kritischer Prozesse	• Vorstellung des Projekts zur Awareness-Bildung • Erhebung der Informationen im Rahmen der BIA auf Basis des Interviewleitfadens Ergebnisse: • Impact-Daten für die Geschäftsprozesse • RTO‘s

Die Kritikalität eines Prozesses wird anhand definierter Impact-Kategorien und Risikoakzeptanz-Schwellen definiert

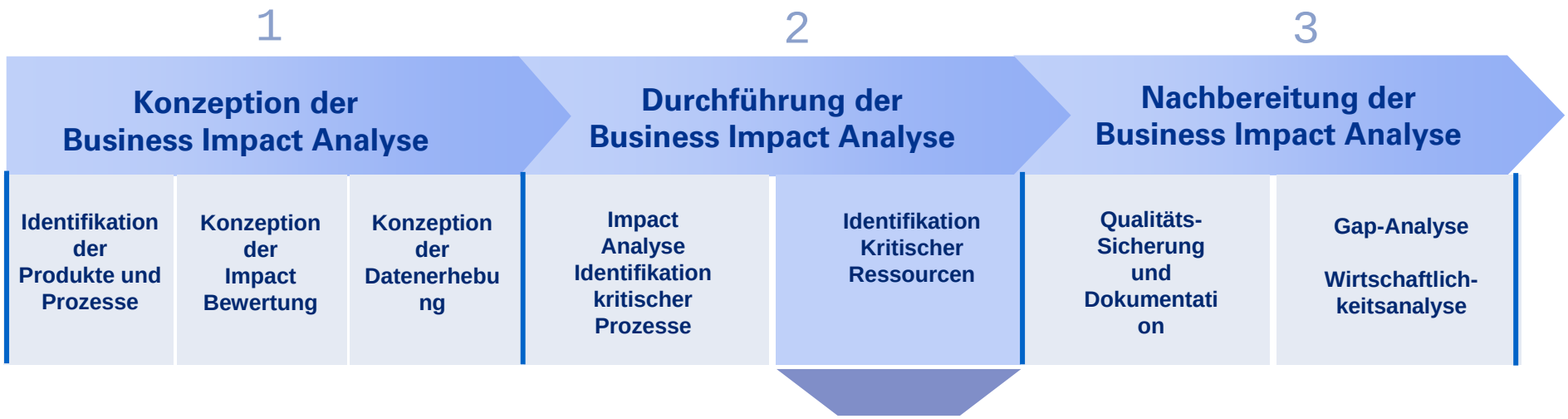
Beispiel: Impact-Analyse für einen Geschäftsprozess



Das BCM muß die Verfügbarkeit der kritischen Wertschöpfungsketten sicherstellen

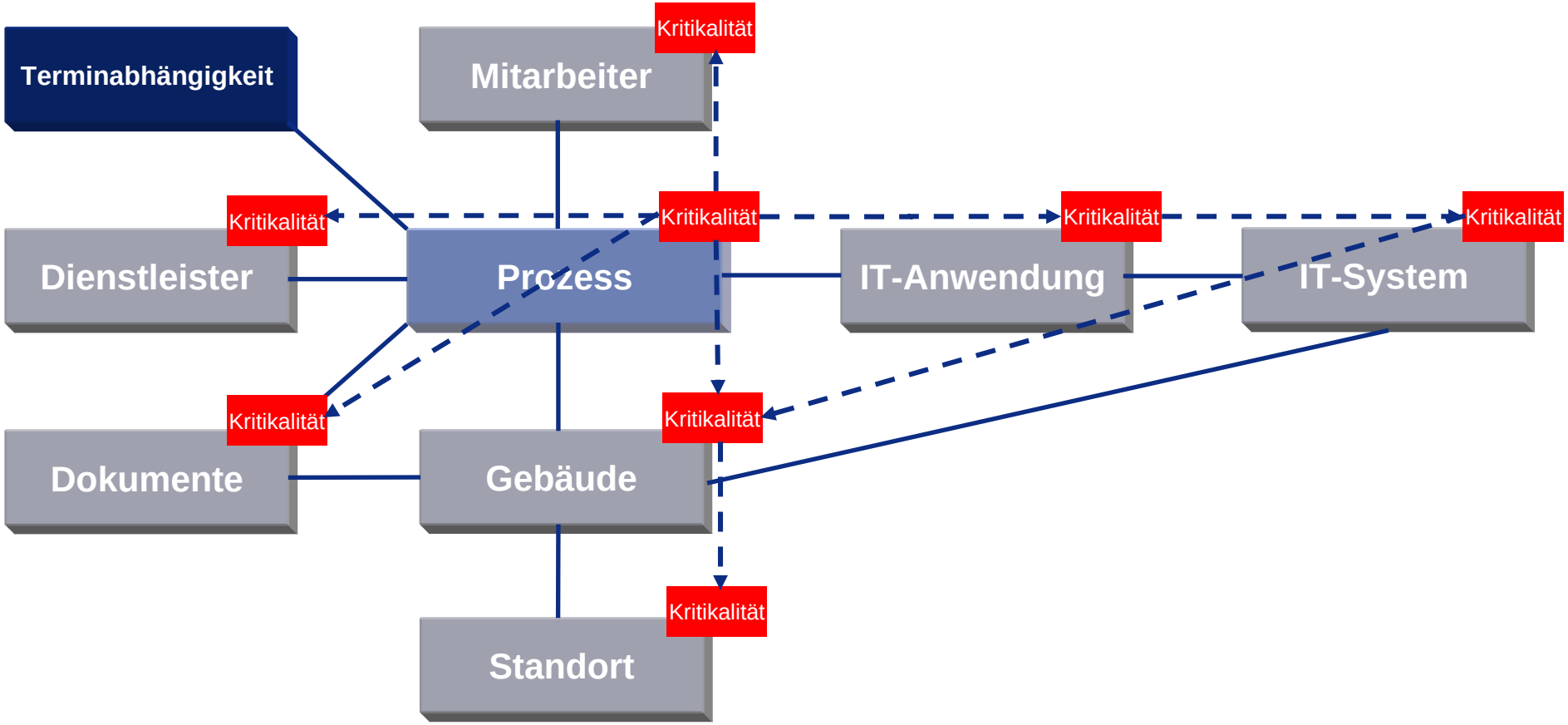


Für die kritischen Prozesse werden in einer Detailerhebung die Ressourcen und deren Kritikalität ermittelt

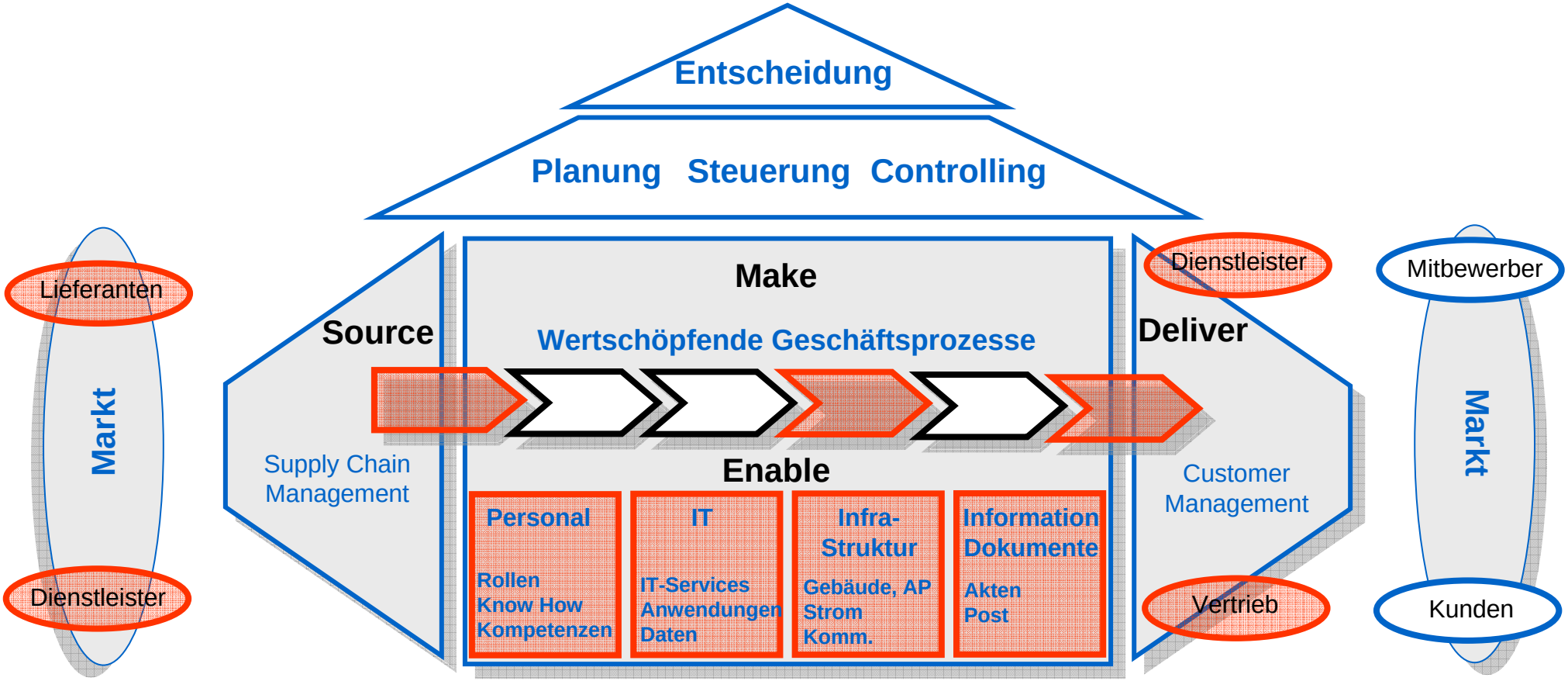


Phase	Inhalt
Identifikation kritischer Ressourcen	• Identifikation der Ressourcen der kritischen Geschäftsprozesse • (regelbasierte) Vererbung der Kritikalität von den Geschäftsprozessen auf die Ressourcen • Mengen und kritische Termine der Geschäftsprozesse Ergebnisse: • Zuordnung der Ressourcen zu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

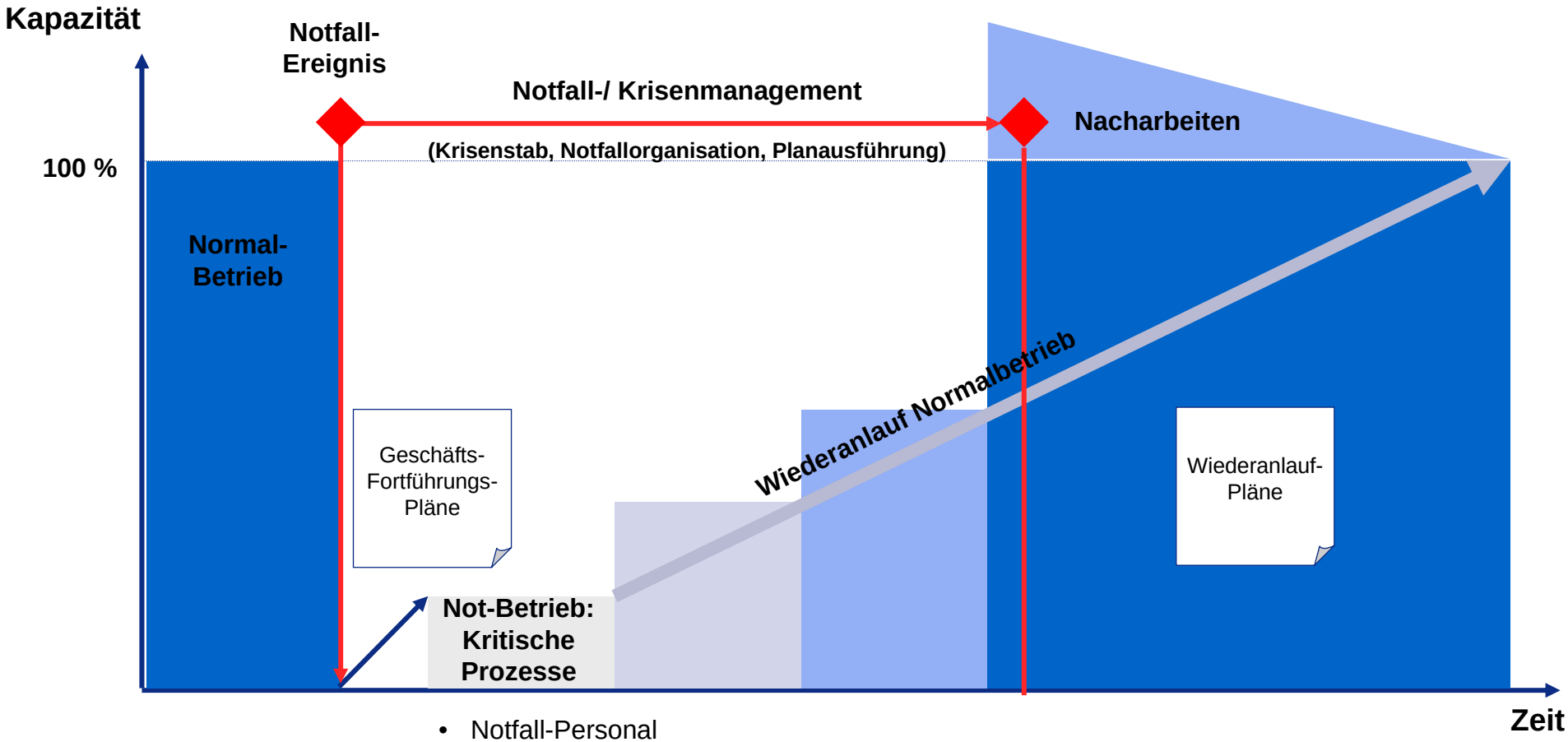
Die Kritikalität (RTO) wird regelbasiert auf die Prozess-Ressourcen vererbt



Für die geschäftskritischen Prozesse werden die Ressourcen für den Notbetrieb identifiziert



Ausgehend vom eingeschränkten Notbetrieb wird der Wiederanlauf geplant

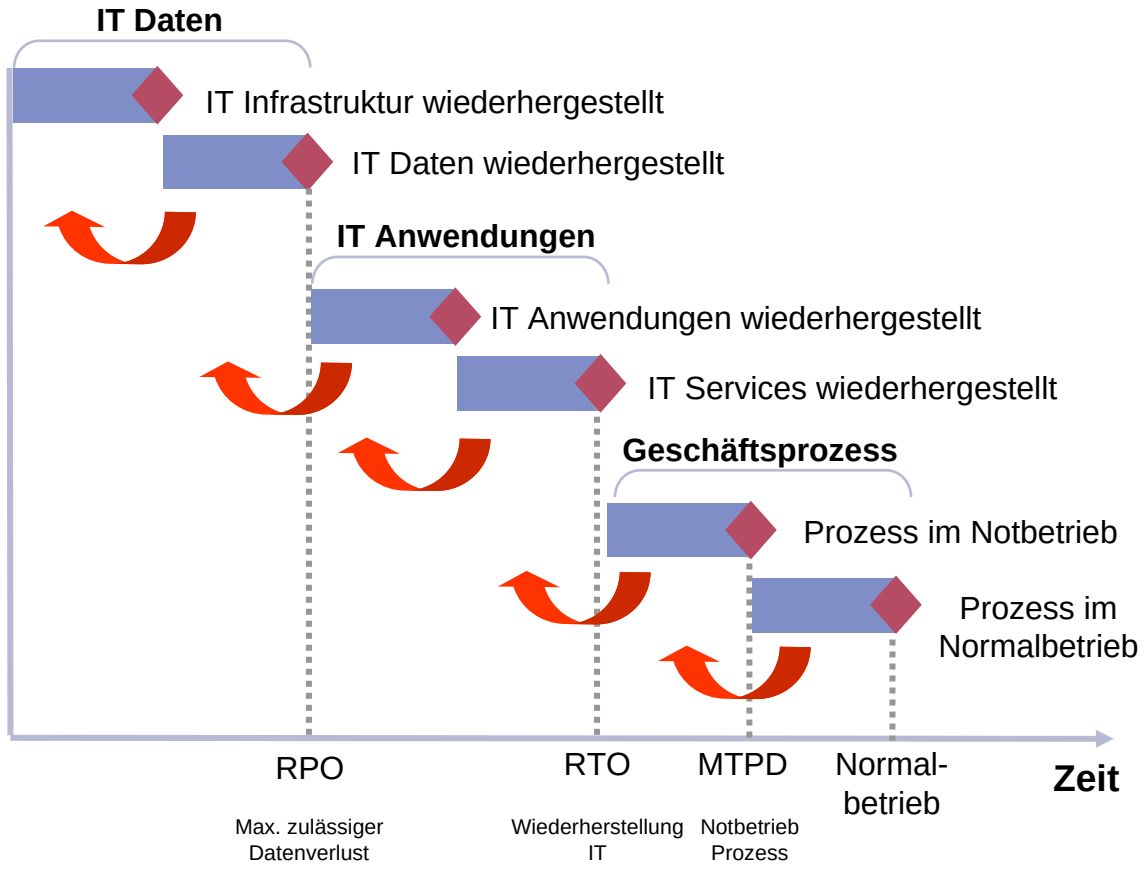


- Notfall-Personal
- Notfall-Arbeitsplätze
- IT-Anwendungen für den Notbetrieb
- Dokumente und Informationen für den Notbetrieb
- Dienstleister für den Notbetrieb

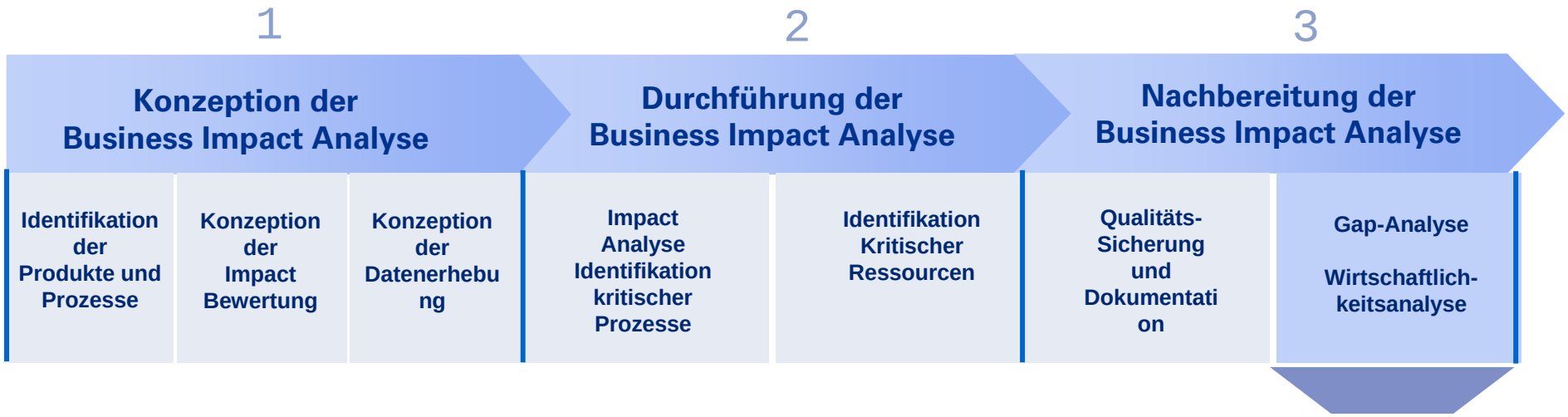
Notbetrieb und Wiederanlauf für einen Geschäftsprozess

Geschäftsprozess "Bonität prüfen"	2 Stunden	0,5 AT	1 AT	2 AT	3 AT	5 AT
IT-Anwendungen						
Anwendung 1	●	○	○	○	○	○
Anwendung 2	○	○	●	○	○	○
Anwendung 3	○	○	●	○	○	○
Anwendung 4	○	○	○	○	●	○
Anwendung 5	○	○	○	○	○	●
Personal	6	6	6	9	12	14
Sachbearbeiter	5	5	5	7	10	12
Kompetenzträger	1	1	1	2	2	2
Dienstleister						
Dienstleister 1	●	○	○	○	○	○
Dienstleister 2	○	○	●	○	○	○
Dokumente						
Kundenakte	●	○	○	○	○	○
KFZ-Briefe	○	○	●	○	○	○
Korrespondenz	○	○	●	○	○	○

Aus den Prozess-Anforderungen werden die IT-Anforderungen (RTO, RPO) abgeleitet



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

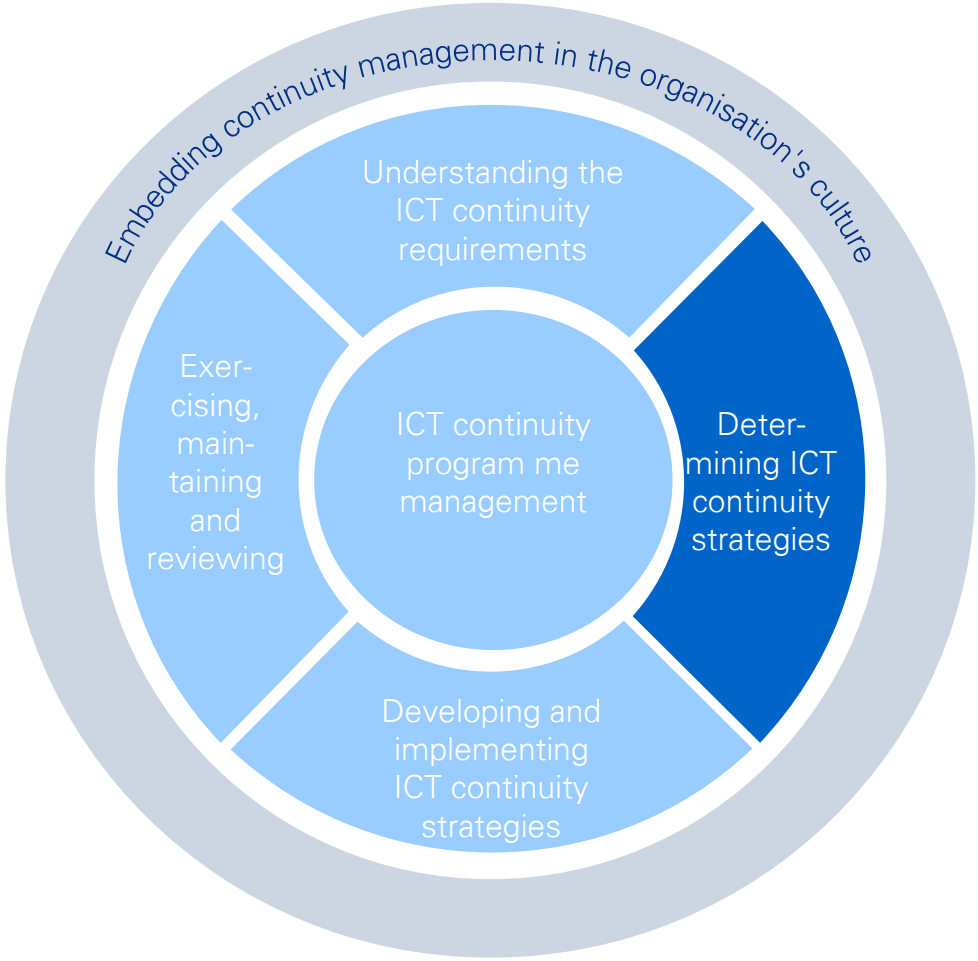


Phase	Inhalt
Wirtschaftlichkeits-Analyse	• Grobe Kostenabschätzung für die Umsetzung der Anforderungen (insbesondere IT und Facility Management) • Balancierung von Anforderungen und Kosten Ergebnisse: • Abgestimmte Anforderungen an Wiederanlauffristen und Notbetriebsanforderungen • Abgestimmter Input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

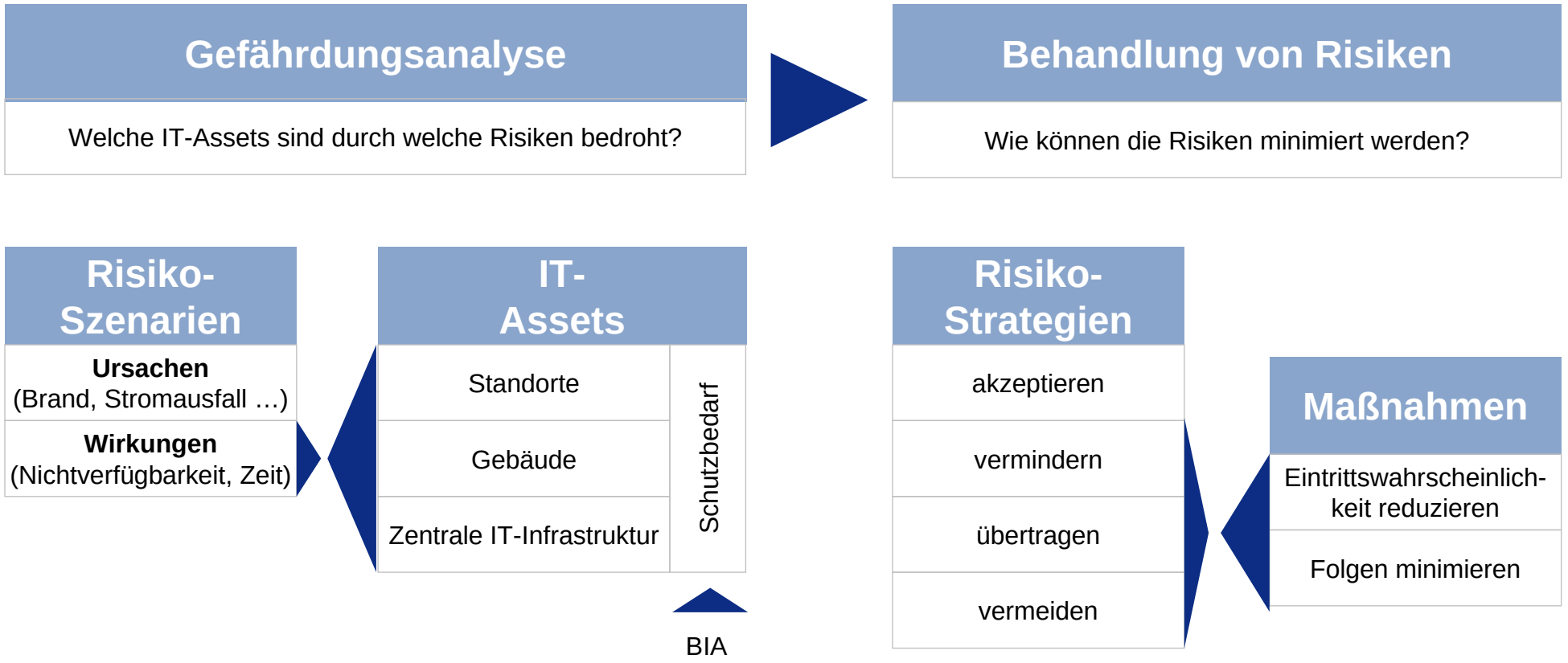
BS 25777-Lifecycle: Continuity-Strategien

Festlegung von ICT Continuity Strategien

- Evaluierung von strategischen Optionen für das ICT Continuity Management
- Die strategischen Optionen sind in Bezug auf die erforderlichen Komponenten zur Aufrechterhaltung und Wiederherstellung der kritischen ICT Services zu ermitteln:
  - Mitarbeiter, Skills
  - Gebäude, Infrastruktur
  - Technologie
  - Daten
  - Dienstleister, Versorger



Ausgehend von der Gefährdungsanalyse für kritische IT-Services und Assets wird die Risikostrategie festgelegt



Aus den Ergebnissen der Business-Impact-Analyse wird der Schutzbedarf abgeleitet

Definition der IT-Assets (Schutzobjekte)

Schutzobjekte

Definition der IT Assets (Personal, zentrale Infrastruktur, Gebäude, Standorte)

Objekt:	Typ:
Server XY	zentrale Infrastruktur

Objekt:	Typ:
RZ Gebäude 1	Gebäude

Impact-Analyse

Impact Analyse

Impact Analyse für IT-Assets Ermittlung der Schadensfolgen über die Zeit	Impact-Bewertung: Gesamtbewertung des Impacts für das IT-Objekt (1: normal 2: hoch 3: sehr hoch)	RTO aus BCM BIAs

Impact-Analyse		Impact Bewertung	RTO aus BIA
		3	2
Dauer Ausfall	**Impact**		
< 4 Stunden	2	2	
< 1 Tag	2	2	
< 2 Tage	3	3	
< 3 Tage	3	3	
< 5 Tage	3	2	
< 10 Tage	3	2	

Impact-Analyse		Impact Bewertung	RTO aus BIA
		3	1
Dauer Ausfall	**Impact**		
< 4 Stunden	2	2	
< 1 Tag	3	3	
< 2 Tage	4	3	
< 3 Tage	4	3	
< 5 Tage	4	3	
< 10 Tage	4	3	

Ableitung des Schutzbedarfs

Schutzbedarf

Abgeleitete Schutzbedarfsklasse für IT-Objekte aus Impact und RTO

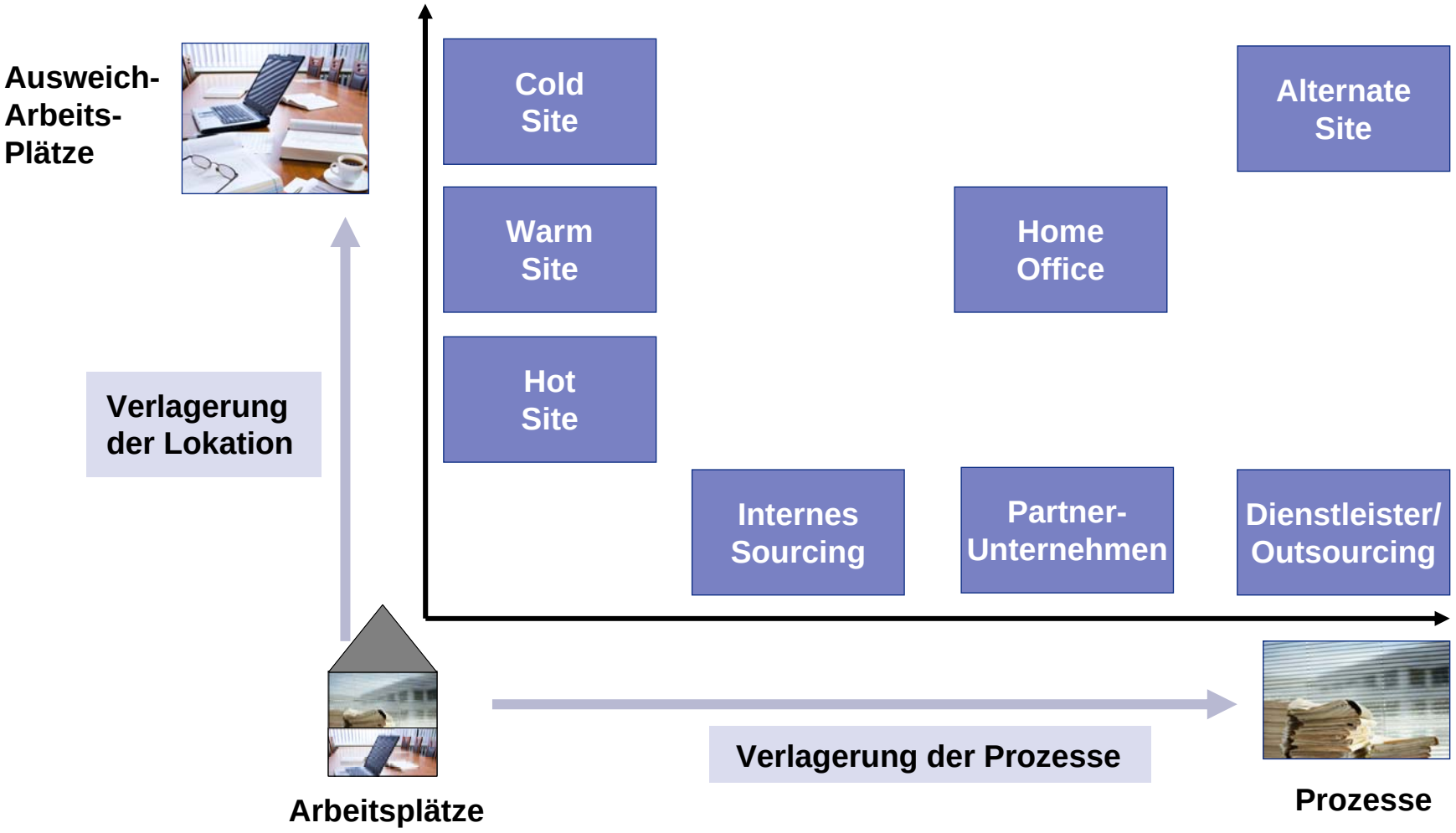
Schutzbedarfsklasse
2

Schutzbedarfsklasse
3

Aus dem Schutzbedarf werden Risikostrategie und Maßnahmen abgeleitet

Schutzbedarf der IT-Assets		Festlegung der Risikostrategie	Analyse der Gefährdungen und Festlegung der Maßnahmen	
Schutzobjekte		**Schutzbedarf**	**Risikostrategie**	**Risikobehandlung**
Definition der IT Assets (Personal, zentrale Infrastruktur, Gebäude, Standorte)		Abgeleitete Schutzbedarfsklasse für IT-Objekte aus Impact und RTO	Festgelegte Risikostrategie für das IT-Objekt	Gefährdungen für das IT-Objekt aus dem Gefährdungskatalog / Maßnahmen für die Gefährdungen aus dem Maßnahmenkatalog
Objekt:	**Typ:**	**Schutzbedarfsklasse**	**Risikostrategie:**	**Gefährdungen** / **Maßnahmen**
Server XY	**zentrale Infrastruktur**	**2**	**Risiko-Reduktion**	
				Gefährdung / **Einzelmaßnahme** / **Status**
				Ausfall des IT-Systems / Ersatzsystem / umgesetzt
Objekt:	**Typ:**	**Schutzbedarfsklasse**	**Risikostrategie:**	**Gefährdungen** / **Maßnahmen**
RZ Gebäude 1	**Gebäude**	**3**	**Risiko-Reduktion**	
				Gefährdung / **Einzelmaßnahme** / **Status**
				Ausfall der internen Stromversorgung / Lokale USV / umgesetzt
				Ausfall interner Versorgungsnetze / Redundanz / umgesetzt

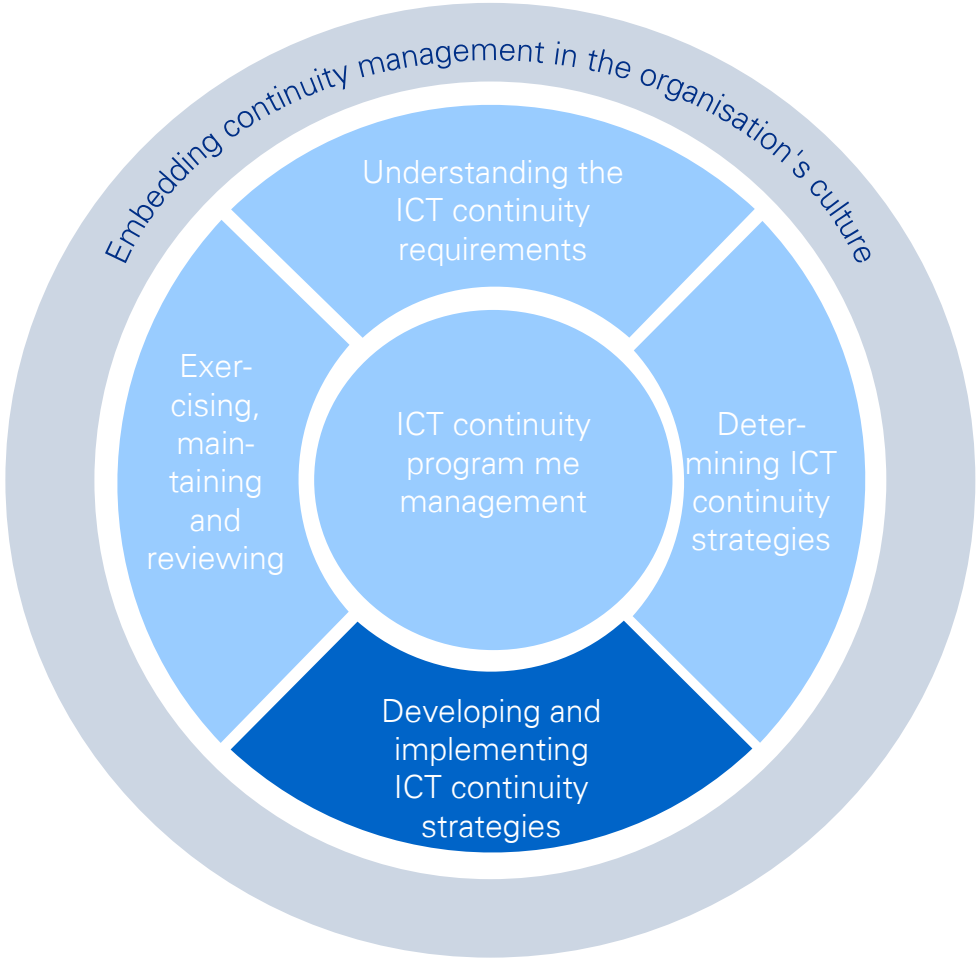
Strategische Optionen für das Szenario „Ausfall Arbeitsplätze“



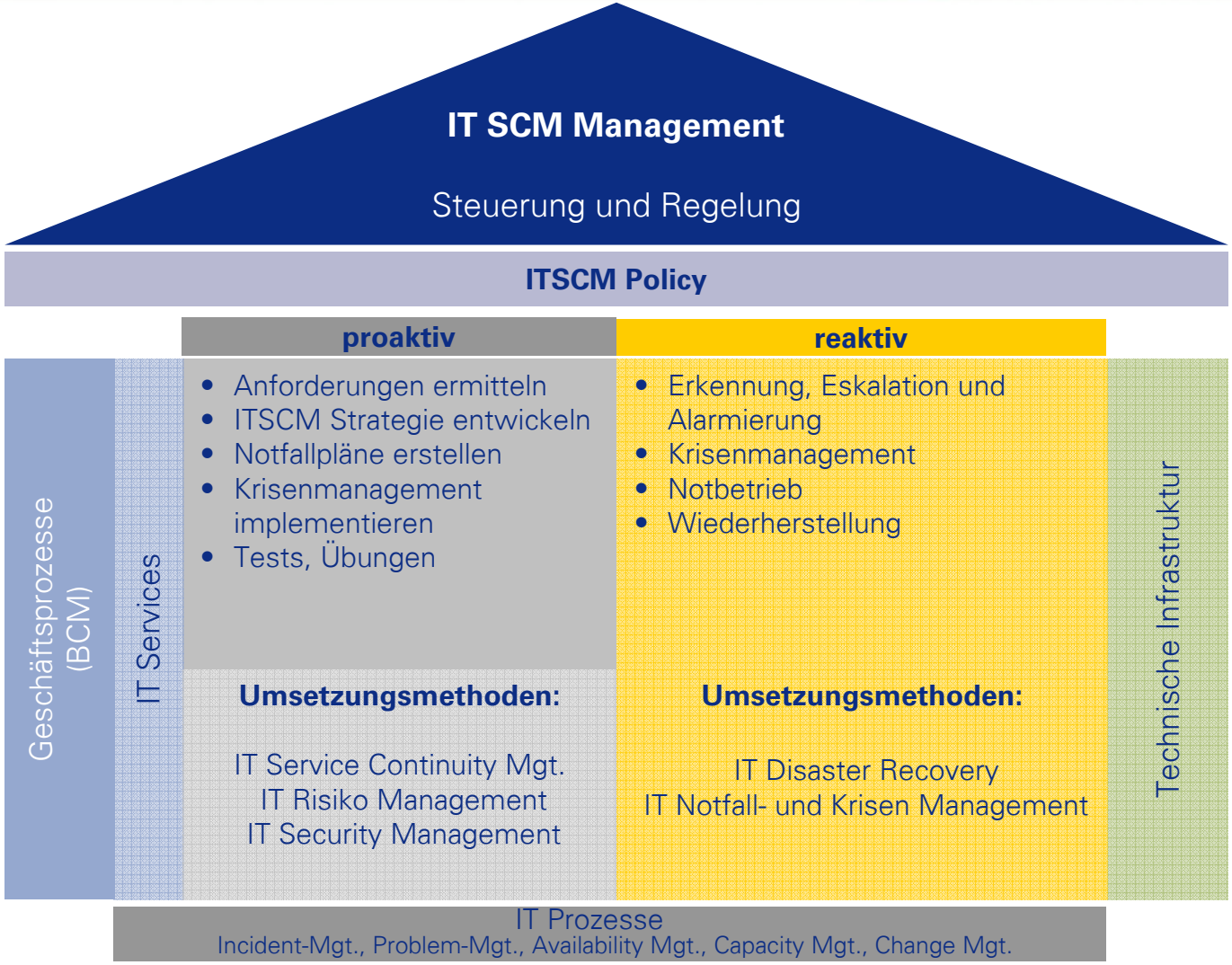
BS 25777-Lifecycle: Implementierung der Strategien

Implementierung der gewählten ICT Continuity Strategien

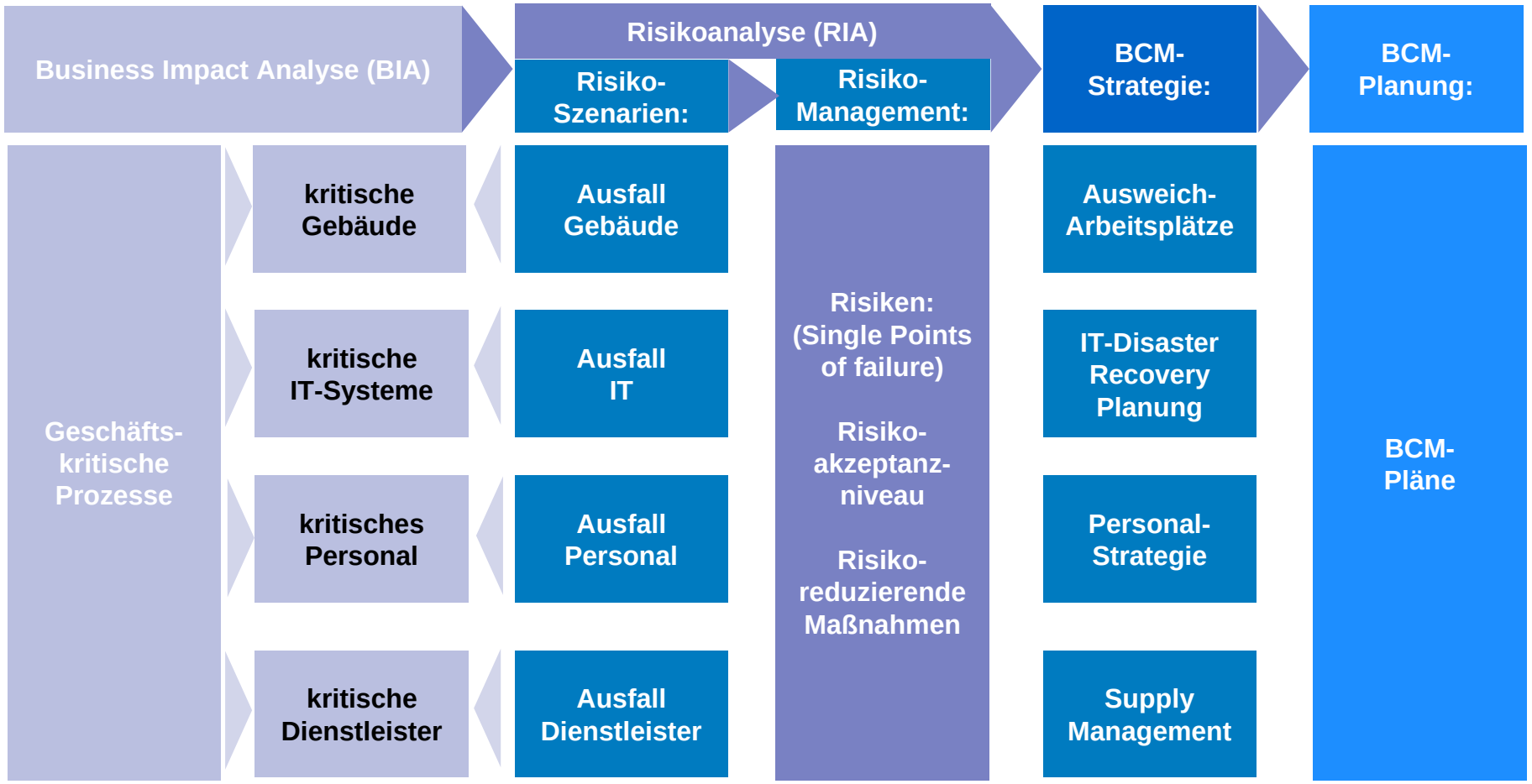
- Dokumentation von Prozessen und Verfahren
- Implementierung von technologischen ICT Strategien (Hot Standby, Warm Standby, Cold Standby, Ship In, kombinierte Verfahren)
- Datensicherungs- und wiederherstellungsverfahren
- Krisenmanagement
- Geschäftsfortführungs- und Wiederanlaufpläne



Die Implementierung des ITSCM beinhaltet einen proaktiven und einen reaktiven Teil



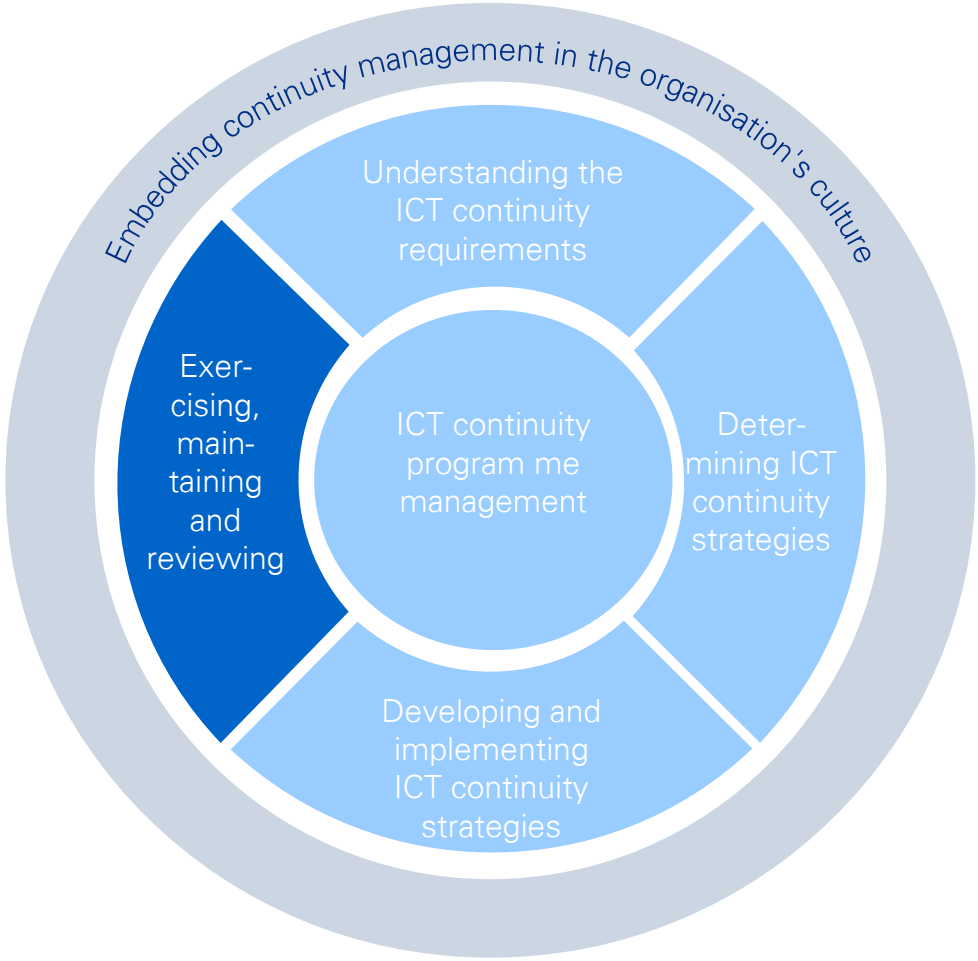
Das IT Service Continuity Management ist integraler Bestandteil des Business Continuity Management



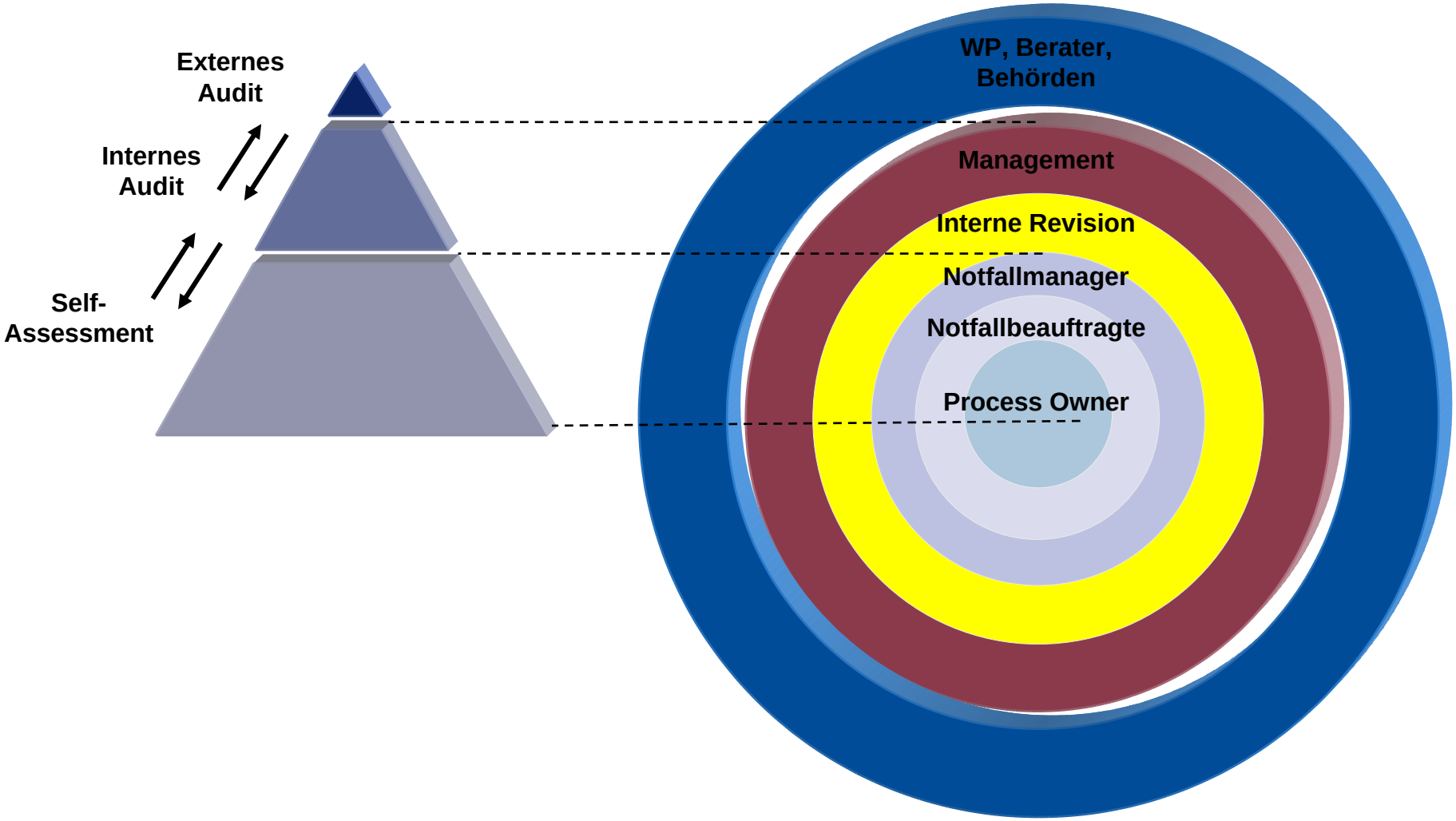
BS 25777-Lifecycle: Übung, Wartung, Audit

Übung, Wartung und Reviews, Audits

- Übungsprogramme
- Change Management
- Interne und externe Audits



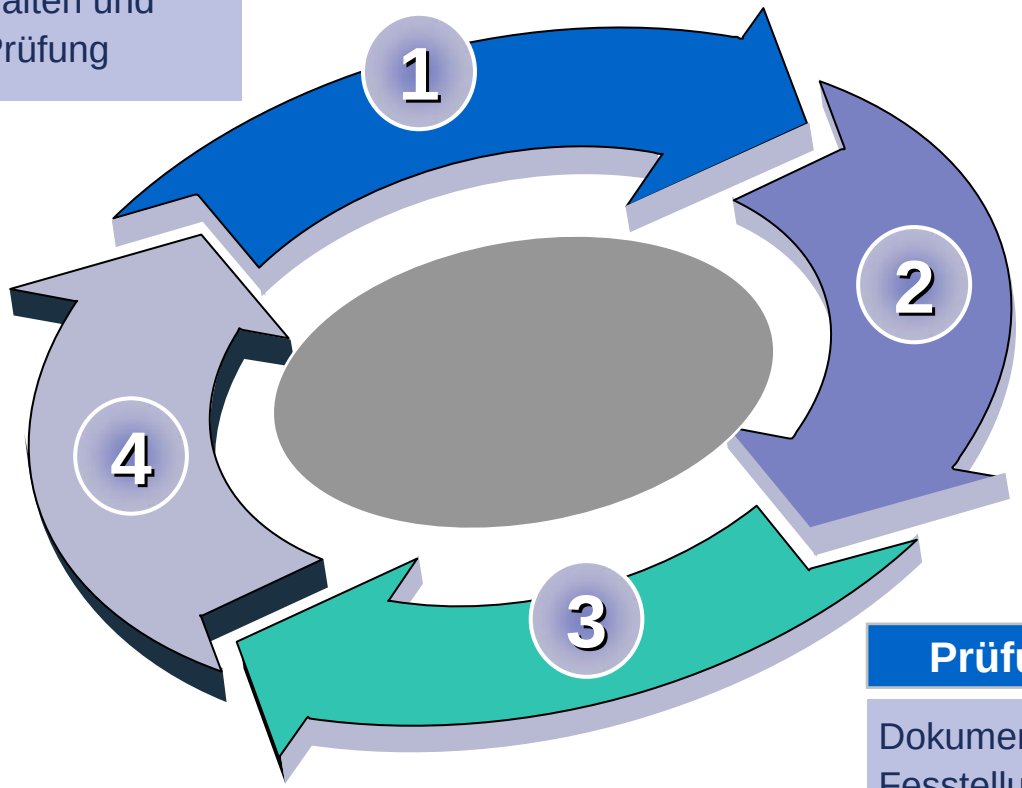
Die Prüfung des ITSCM ist ein abgestuftes und abgestimmtes Verfahren



Der 4-stufige Audit-Zyklus für das ITSCM

ITSCM Prüfungsplan

Festlegung von Zielen, Umfang, Inhalten und Rollen der Prüfung



ITSCM Prüfung

Prüfung des BCM gegen definierte Standards und Performance Indikatoren

Maßnahmen

Monitoring der Umsetzung der Maßnahmen, Dokumentation

Prüfungsbericht

Dokumentation der Fesstellungen und des Handlungsbedarfs

Vielen Dank für Ihre Aufmerksamkeit!

Matthias Hämmerle MBCI
Senior Manager
Advisory

Marie-Curie-Strasse 30
D-60439 Frankfurt/Main
mhaemmerle@kpmg.com

Tel. 49 (69) 95 87 - 4960
Fax 49 (1802) 11991 9251
Mobile 49 (173) 576 4211

KPMG Deutsche Treuhand-Gesellschaft Aktiengesellschaft
Wirtschaftsprüfungsgesellschaft • Member of KPMG International