

PERSICON

Information Risk Management
Consultancy

Business Continuity Management

Herausforderungen und Lösungen

Mittwoch, 6. Februar 2008

Knud Brandis

- Jurist, Master of Business Administration (MBA)
- Certified Information System Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Certified Information System Auditor (CISA)
- Mitautor BSI IT-Grundschutzhandbuch
- Lizenziertes BSI IT-Grundschutzauditor
- ISO 27001 Auditor (BSI & TÜV)



PERSICON

- Prüfungs- und Beratungsgesellschaft auf den Gebieten Risikomanagement und Informationssicherheit
- Spezialist für [Governance](#) | [Compliance](#) | [Security](#)
- Spin-off einer internationalen führenden WP-Gesellschaft
- Niederlassungen in Berlin, Potsdam, New York und Frankfurt
- 20 Mitarbeiter in Deutschland
- Kunden: Deutsche Post, E.ON, ThyssenKrupp, RWE, ARD, Staatskanzlei, BSI...
- [PERSICON AG](#) | [Friedrichstraße 188](#) | [10117 Berlin](#)

PERSICON Leistungsschwerpunkte

- IT-Sicherheitszertifizierungen (ISO 27001, BSI IT-Grundschutz...)
- Ordnungsmäßigkeitstestierungen (SAS 70, IDW...)
- Implementierung Interner Kontrollsysteme (IKS)
- Co- & Outsourcing Interne Revision
- IT-Notfallvorsorge / Business Continuity Management
- IT-Security Audits & IT-Sicherheitskonzeption
- Schadenspotential- und Risikoanalysen
- Stellung des externen Datenschutzbeauftragten
- Trainings & Coaching...

Agenda

- Einführung
- Prozesse, IT-Services und Ressourcen
- Standards und Richtlinien
- Good Practice Guidelines - The Business Continuity Institute (BCI)
- Umsetzung in der Praxis

Business Continuity Management

EINFÜHRUNG

Einführung

Mittwoch, 6. Februar 2008

PERSICON

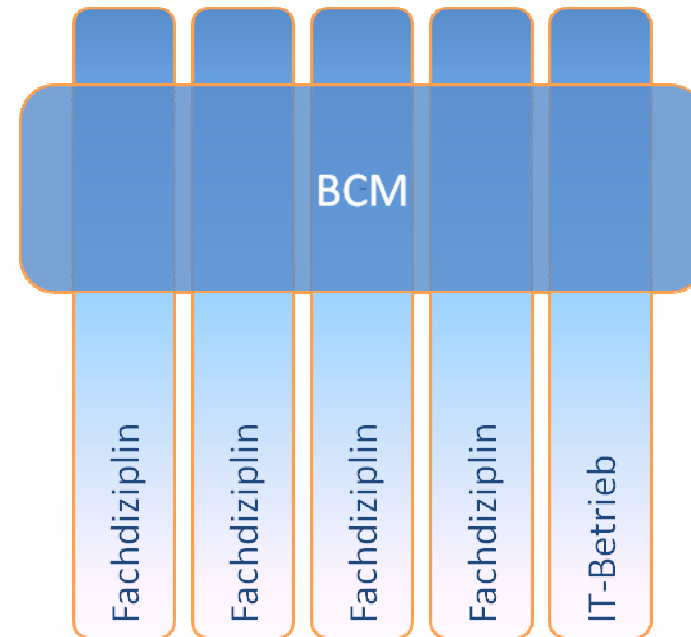
6

Der Begriff „Business Continuity Management (BCM)“

- BCM ist ein Managementprozess, welcher gewährleistet,
 - das kritische Geschäftsprozesse
 - auch in Not- und Krisensituationen verfügbar sind und
 - eine kontrollierte Fortführung der Geschäftstätigkeit ermöglicht.

Einordnung des BCM

„BCM wird vollständig als eingebetteter Managementprozess in die Organisation integriert und ist integraler Bestandteil des Unternehmens.“



ohne Business Continuity Management drohen...

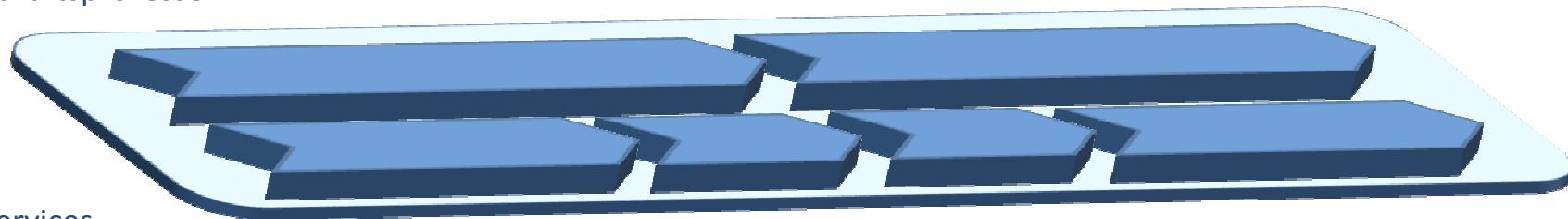
- unbekannte oder nicht kalkulierte **Risiken** für den Geschäftsbetrieb
- eine **nicht kontrollierte** Krisenreaktion/Wiederaufbau bei Ausfällen
- unnötige **Kosten/Ausfallzeiten**
- **Schäden** bis zum Totalverlust der Geschäftsfähigkeit und des Unternehmens
- **Haftung**
- Einhaltung gesetzlicher und regulatorischer Anforderungen an das ganzheitliche Risikomanagement

Business Continuity Management

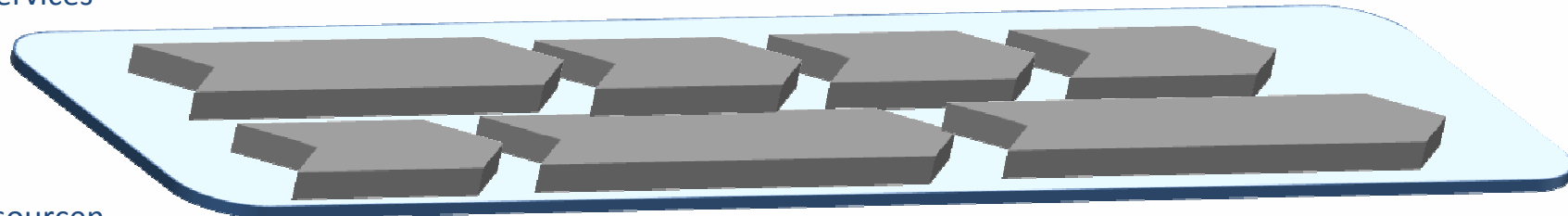
PROZESSE, IT-SERVICES UND RESSOURCEN

Prozesse, IT-Services und Ressourcen

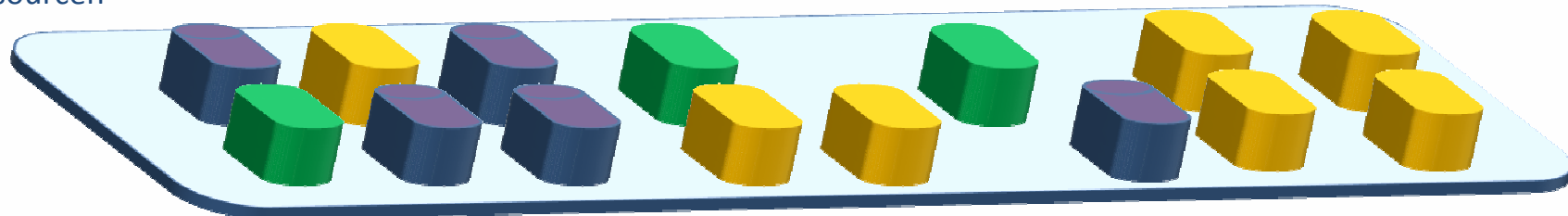
Geschäftsprozesse



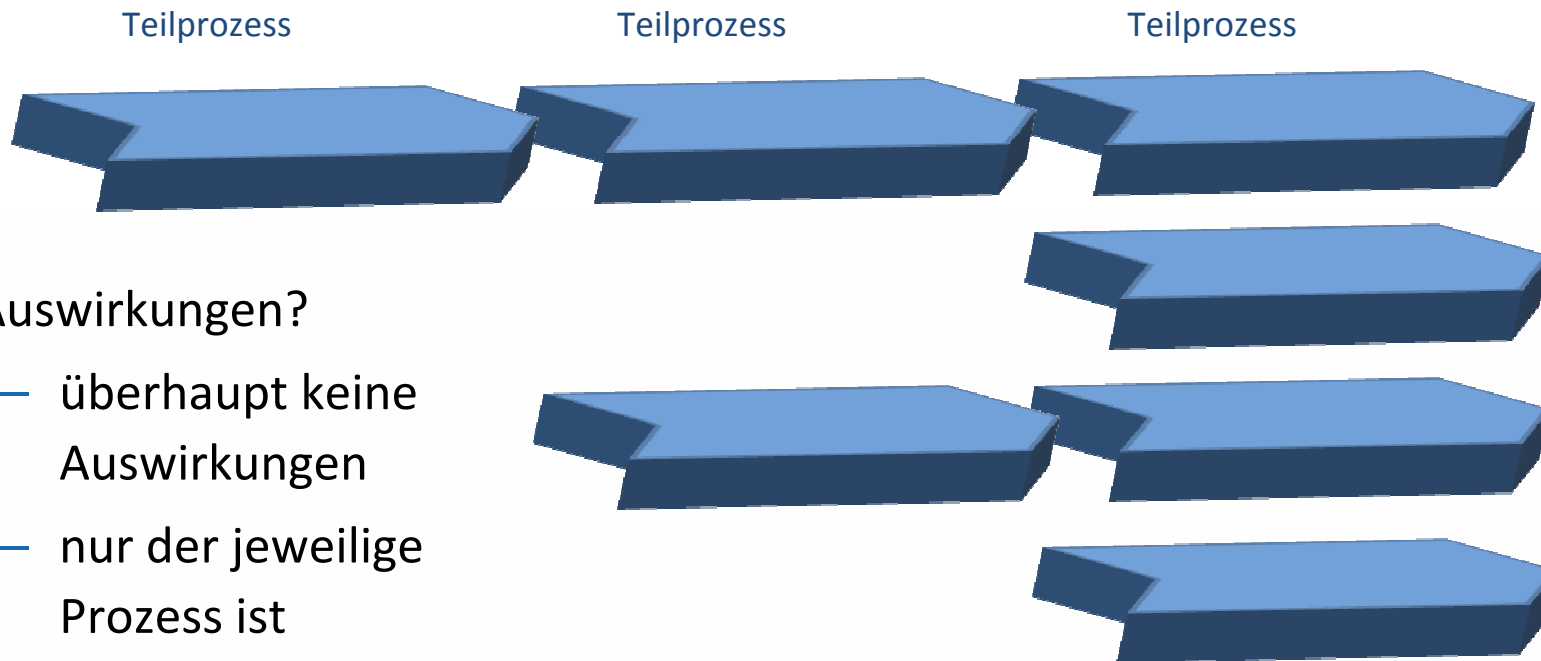
IT-Services



Ressourcen

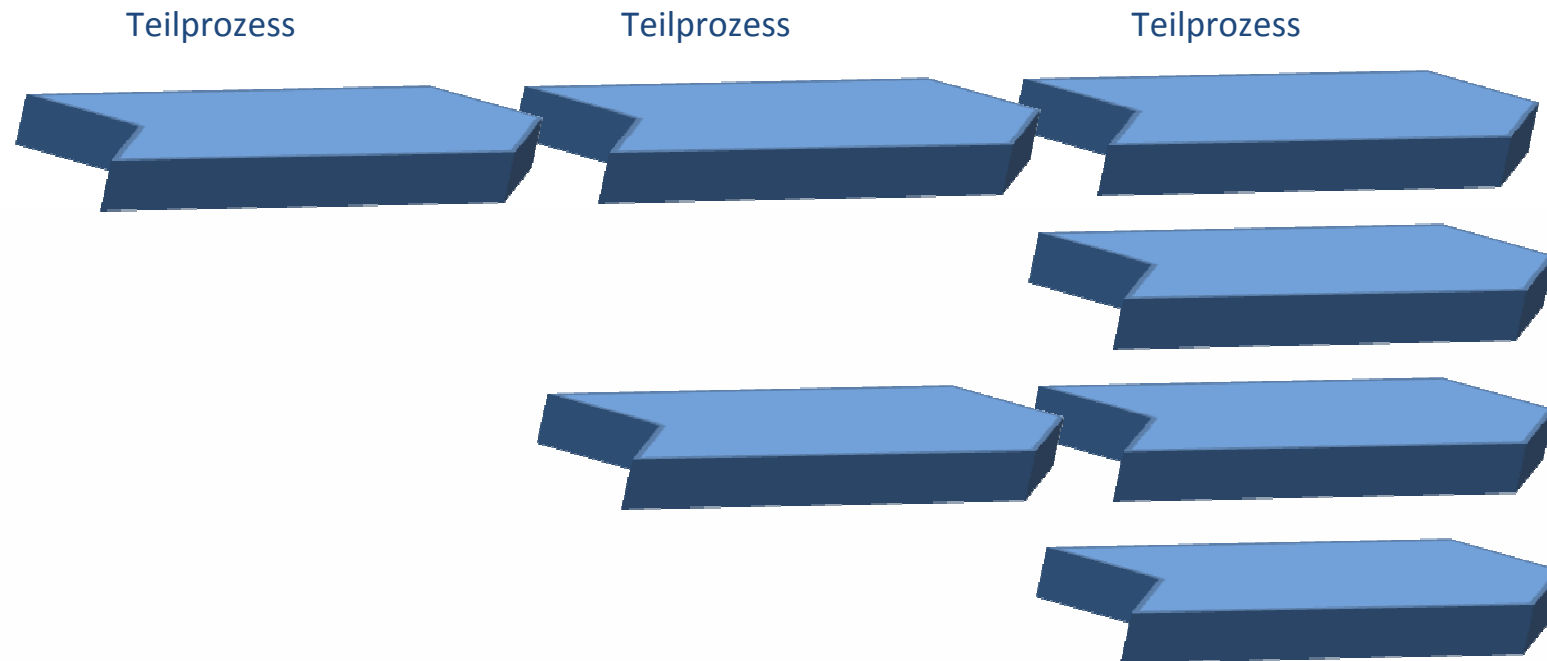


Abhängigkeit der Prozesse untereinander

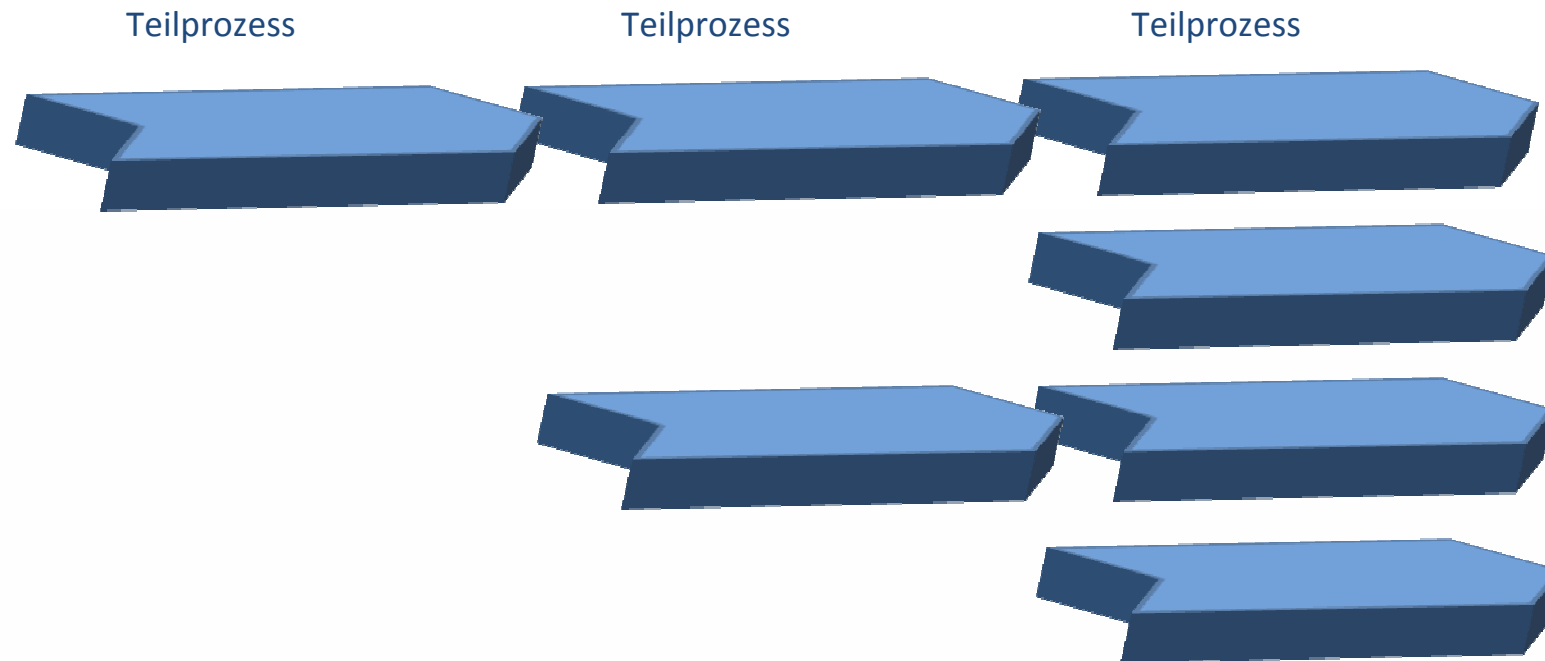


- Auswirkungen?
 - überhaupt keine Auswirkungen
 - nur der jeweilige Prozess ist betroffen
 - ...

Abhängigkeit: Input blockiert



Abhängigkeit: Output blockiert



Prozesse: Wodurch ergibt sich deren Kritikalität?

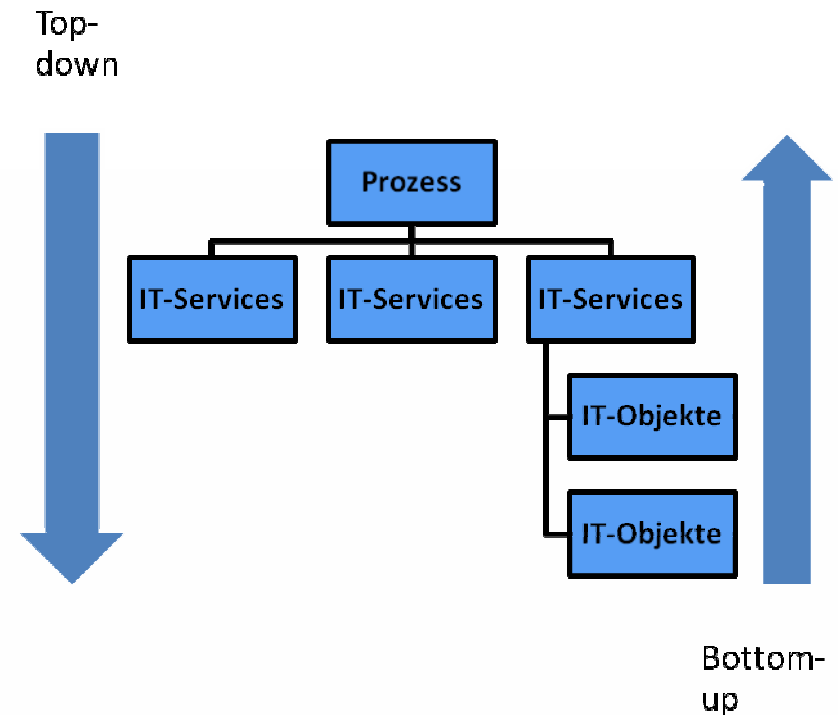
- Abhängigkeiten
 - direkte Abhängigkeit der Prozesse zu Unternehmenszielen
 - Hilfsprozesse, von denen die Unternehmensziele (indirekt) abhängig sind
 - Welche Störungen/Ausfälle der Prozesse wirken wie schnell und wie stark aus (Business Impact)?
- Betrachtung der Prozesse z.B. nach
 - Eingangsgrößen und Ausgangsgrößen (Input/Output bzw. Kosten/Gewinn)
 - Abhängigkeiten der Prozesse untereinander (blockieren von vor- oder nachgelagerten Prozessen)

Kritische Prozesse – mögliche Schäden

- Frage: Welche Schäden sind denkbar?
 - grundsätzlich sind Schäden (auch) finanzieller Art
- weitere Beispiele:
 - Image
 - Gesetzesanforderungen/Vertragsstrafen
 - Lieferung (Lieferverzug, Schlechtlieferung)
 - Wachstum
 - Marktchancen
 - und ggf. Leben und Gesundheit(!)

Top-down vs. Bottom-up

- Top-down Ansatz (aus Sicht der Prozesse)
- Bottom-up Ansatz (aus der IT-Systeme)
- kombinierter Ansatz



Business Continuity Management

STANDARDS UND RICHTLINIEN

Standards und Richtlinien

Mittwoch, 6. Februar 2008

PERSICON

18

British Standard

- BS 25999-1:2006
 - Code of Practice for Business Continuity Management
 - ersetzt die frühere Publicly Available Specification PAS 56:2003, „Guide to Business Continuity Management“
- BS 25999-2:2007
 - Specification for Business Continuity Management (Anforderungen an ein Business Continuity Management System -BCMS-)
- The Business Continuity Institute (BCI): Good Practice Guidelines
 - A Management Guide to Implementing Global Good Practice in Business Continuity Management (Stand 03/2007)

ISO und Singapore Standard

- ISO/IEC 27006
 - Guideline for information and communications technology disaster recovery services
- Singapore Standard SS507:2004
 - Business Continuity/Disaster Recovery Service Provider
 - Status: „Under Revision“

Weitere BCM Standards

- NFPA 1600 (The North American business continuity standard)
 - Standard on Disaster/Emergency Management and Business Continuity Programs (Stand 2007)
- HB 221:2004 Business Continuity Management (Australia)
- Prudential Standard APS 232 Business Continuity Management (Australia)
- Financial Services Authority (FSA) - Business Continuity Management Practice Guide (UK)

Diverse Standards mit BCM-Inhalten

- ITIL (IT Infrastructure Library)
 - Availability Management
 - Continuity Management
- IT-Grundschatz
 - B 1.3 Notfallvorsorge-Konzept
 - Neuer IT-Grundschatz Baustein wird sich an BS 25999 orientieren
 - Hierzu wird weiterhin der IT-Grundschatz Standard 100-4 veroffentlicht (aktuell verzogert)

Diverse Standards mit BCM-Inhalten

- COBIT
 - DS4.1 - IT Continuity Framework
 - DS4.6 - IT Continuity Plan Training
 - DS4.7 - Distribution of the IT Continuity Plan
 - DS4.10 - Post-resumption Review
 - DS12.1 - Site Selection and Layout
- NIST Special 800-34
 - Contingency Planning Guide for Information Technology Systems
- PAS 77:2006
 - IT Service Continuity Management

Business Continuity Management

GOOD PRACTICE GUIDELINES

THE BUSINESS CONTINUITY INSTITUTE (BCI)

BCM Policy & Programme Management

BCM Policy

- dokumentierte Aussage zum Stellenwert des BCM durch die Geschäftsführung
- Voraussetzung ist die Kenntnis der Ziele der Organisation und wie diese Ziele umgesetzt werden
- Aufbau der Policy
- Definition des BCM-Scopes
- Berücksichtigung ausgelagerter Prozesse (outsourced Activities)

BCM Policy & Programme Management

Programme Management

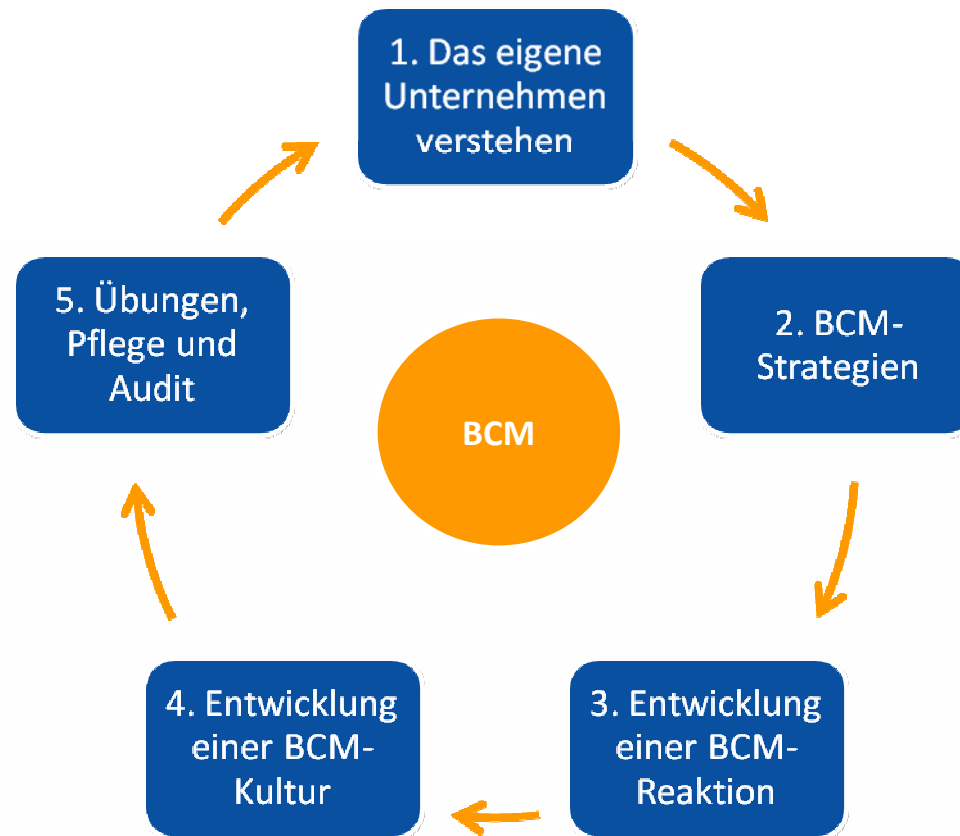
- Verantwortlichkeiten zuweisen
- Implementierung in die Organisation
 - Sensibilisierungsmaßnahmen
(BCM-Ziele, Durchführung der BIA etc.)
- Projekt Management
- Ongoing BC Management (Weiterführung des BCM nach Projektende)
- Dokumentation
 - Form der Dokumentation (Online, Offline, Printversion)
 - Standards vorgeben und Prozess etablieren
- Incident Readiness & Response

Das Business Continuity Management-Programm

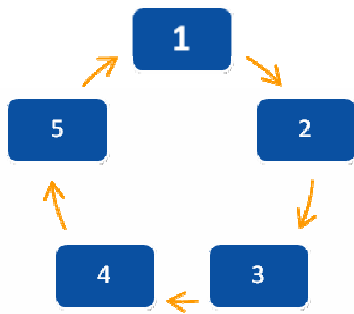
- Phase 1: Das eigene Unternehmen verstehen
- Phase 2: Business Continuity Management-Strategien
- Phase 3: Entwicklung und Implementierung einer BCM-Reaktion
- Phase 4: Entwicklung einer BCM-Kultur
- Phase 5: Übungen, Pflege und Audit

Quelle: THE BUSINESS CONTINUITY INSTITUTE, BUSINESS CONTINUITY MANAGEMENT, GOOD PRACTICE-RICHTLINIEN

Der Business Continuity Management-Lebenszyklus

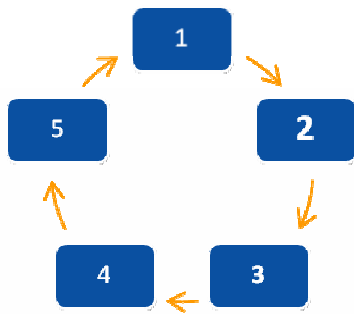


Phase 1: Das eigene Unternehmen verstehen



- Organisationsstrategie
 - Ziele der Organisation und deren Umsetzung
- Business Impact Analyse (BIA)
 - Analyse (z.B. Interviews): Welche Prozesse sind kritisch für diese Ziele?
 - Maximal tolerierbarer Ausfall (MTO - Maximum Tolerable Outage)
 - erforderlicher Zeitpunkt des letzten Standes der Daten (RPO - Recovery Point Objective)
- Risikobeurteilung
 - Wahrscheinlichkeit und Auswirkungen

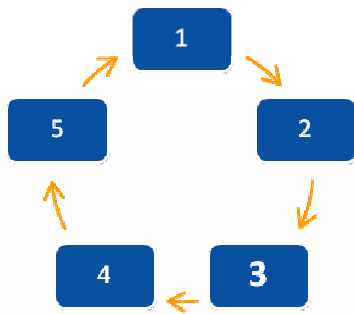
Phase 2: BCM-Strategien



Grundsätzliche Business Continuity-Managementstrategien

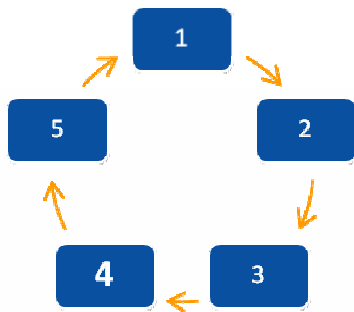
- alternative Betriebsmethoden, um nach einem Ausfall die Prozesse gemäß den Vorgaben aufrechtzuerhalten bzw. wiederherzustellen (Priorität und Zeitraum)
 - vorhandene Infrastruktur umwidmen, Telearbeit, angemietete Räume, Ausweich-RZ etc.
- Absicherung der kritischen Prozessen durch Schutzmaßnahmen
- Prozesse anpassen
- Outsourcing
- ...

Phase 3: Entwicklung einer BCM-Reaktion



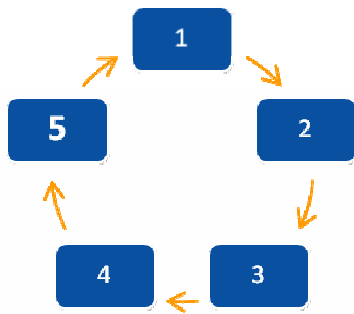
- Krisenmanagement-Plan (strategisch)
 - Verantwortliche, Krisenstab
 - Krisenkommunikation
 - Krisenreaktion
- Business Continuity-Pläne (taktisch)
 - Reaktion auf BCM-Vorfall: Handlungsanweisungen zu Sofortmaßnahmen und Notbetrieb
 - Fortführung innerhalb der MTO
- Wiederaufnahmepläne (betrieblich)
 - Wiederherstellung der Prozesse und Ressourcen vom Notbetrieb zum Regelbetrieb

Phase 4: Entwicklung einer BCM-Kultur



- Beurteilung der BCM-Awareness
 - Beobachtung/Interviews
 - Feedback der Mitarbeiter
- Entwicklung einer BCM-Kultur
 - Anerkennung der BCM-Policy
 - „Vorleben“ der Leitungsebenen
 - Schulungen zur Sensibilisierung
- Überwachung des kulturellen Wandels
 - BCM-Awareness ausreichend?
 - Neue/weitere Anforderungen

Phase 5: Übungen, Pflege und Audit



- Übungen
 - Voraussetzung: realistische Bedingungen
 - Bewertung der aktuellen BCM-Kompetenz der Organisation
 - Effektivität und Effizienz
 - mögliche Verbesserungspotentiale
 - Erfahrungen sammeln und Teamwork
- Pflege
- Audit
 - unabhängige Überprüfung und Bewertung des BCM
 - transparenter Nachweis

Business Continuity Management

UMSETZUNG IN DER PRAXIS

Umsetzung in der Praxis

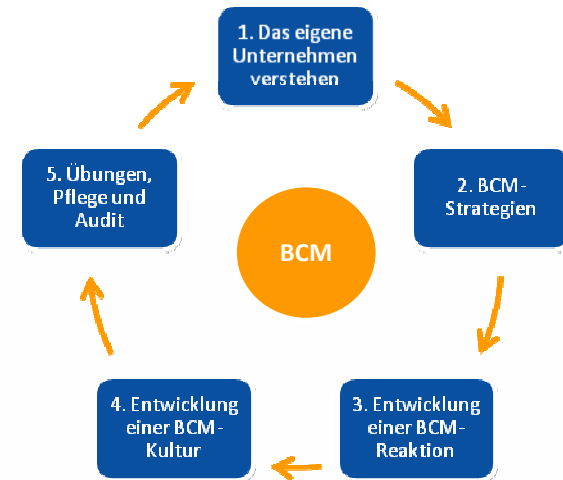
Mittwoch, 6. Februar 2008

PERSICON

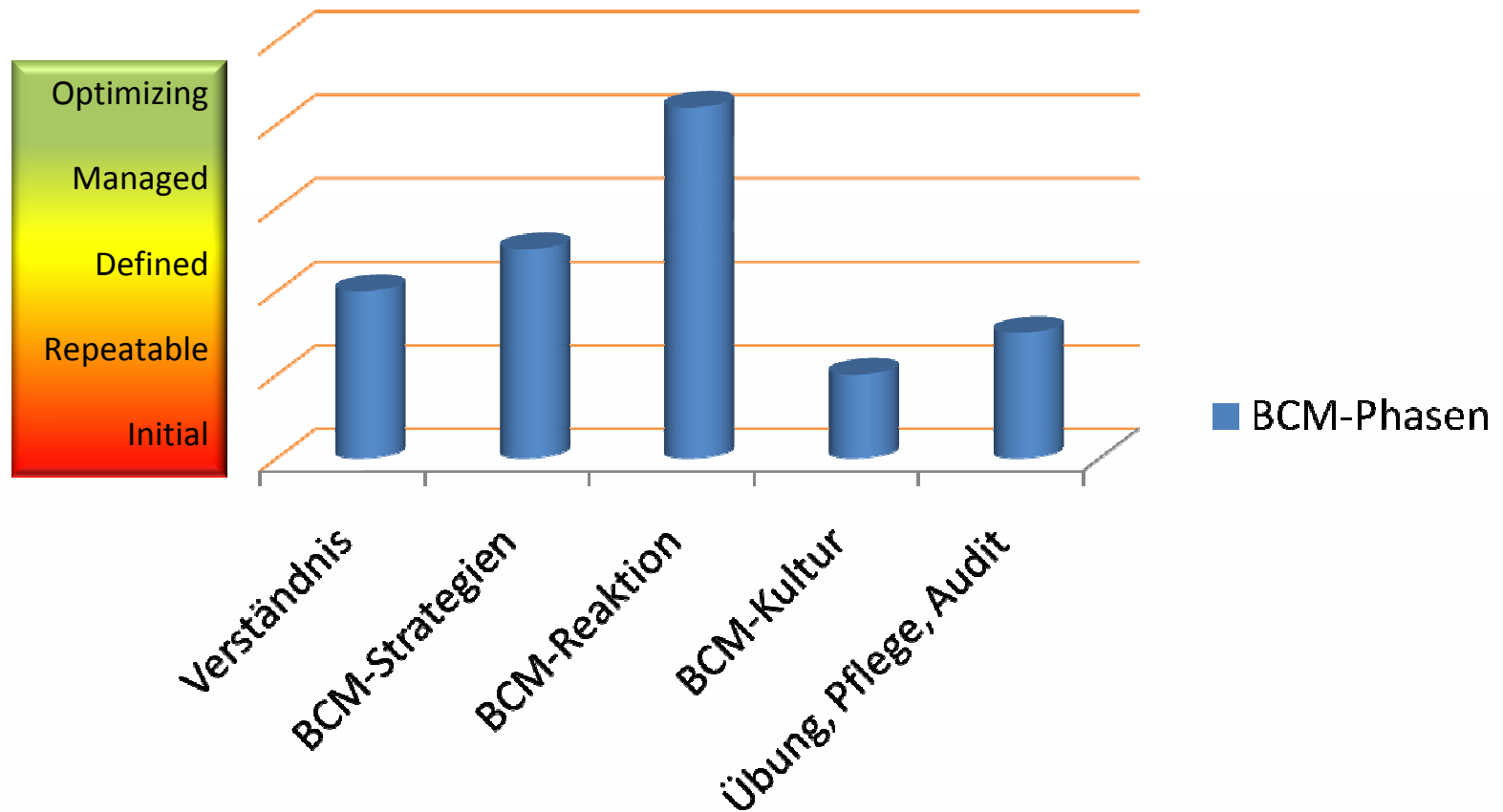
34

BCM-Projekte

- Projektstart in grundsätzlich allen Phasen des BCM-Lifecycles möglich
 - optimalerweise in Analysephase oder Übungen/Audit
- Überprüfung des Reifegrades des vorhandenen BCM
 - von „intial“ bis „optimizing“



Reifegrad des BCM-Programms



Erfolgsfaktoren in BCM-Projekten

- objektive Anforderungen klären
- subjektive Motivation und Erwartungen eruieren
- Unterstützung der Geschäftsführung sicherstellen,
 - ggf. sensibilisieren
- BCM-Policy mit der Geschäftsführung erarbeiten und verabschieden
- Schnittstellen/Synergien analysieren
 - Wer sind die Ansprechpartner?
 - Beispiel: IT-Sicherheit und BCM-Relevanz

Konsequenzen

- Erkennen der kritischen Prozesse für die Geschäftsziele und welche Risiken bestehen
 - **Konsequenz:** Die Möglichkeit Risiken angemessen zu steuern
- Ganzheitliche Bewertung des Unternehmens
 - **Konsequenz:** (erster?) Gesamtüberblick über das Unternehmen
 - **Konsequenz:** Optimierungspotentiale werden in der gesamten Organisation identifiziert
- Ähnliche Anforderungen mit anderen Gesetzen und Normen
 - **Konsequenz:** Synergieeffekte bieten effiziente Möglichkeiten für weitere positive Entwicklungen

Welche Fragen haben Sie?



Fragen

Mittwoch, 6. Februar 2008

PERSICON

39

Vielen Dank für Ihre Aufmerksamkeit

Knud Brandis

www.persicon.com

kbrandis@persicon.com

PERSICON AG | Friedrichstraße 188 | 10117 Berlin