

# **BS 25999**

## **Standard für Business Continuity Management**

Dipl.-Ing. Tobias Timmler





- Unternehmensstandort Hamburg
- gegründet 1.4. 2005
- langjährige Beratungserfahrungen
  - Business Continuity
  - Information Security
  - Service Quality
- bei Großunternehmen und Mittelstand
  - Banken und Versicherungen
  - Industrie und Handel
  - Logistik- und Medienunternehmen
  - Behörden
- Wir helfen unseren Kunden,
  - ihre Geschäftsfähigkeit gegen operationelle Risiken abzusichern
  - und so ihre Wettbewerbsfähigkeit zu verbessern.





# Agenda

---

- Business Continuity Management (BCM) – Definition
- Inhalte des Standard BS 25999-1:2006
- Was kommt im Standard BS 25999-2:2007
- Was bedeutet Audit bzw. Zertifizierung im Bereich BCM für ein Unternehmen
- BS 25999 - Resumée



# Der neue Standard BS 25999-1:2006

- Nationaler britischer Standard
  - keine ISO-Norm, kein ÖNORM, keine DIN
- Leitfaden für Business Continuity Management
- Entwickelt aus PAS 56:2003
  - (BCI Leitlinie, Business Continuity Institute, [www.thebci.org](http://www.thebci.org))
- Veröffentlicht im November 2006 vom BSI
  - nur in englisch verfügbar
- Bezugsquelle:  
BSI British Standards Institute, 389 Chiswick High Road,  
London, W4 4AL, UK  
[www.bsi-global.com](http://www.bsi-global.com)  
£ 90.00



# Business Continuity Management - Definition

BS 25999:

- BCM ist eine ganzheitliche Managementmethode zur Aufrechterhaltung des Geschäftsbetriebs in einem akzeptablen Mindestmaß nach Eintritt einer Geschäftsunterbrechung.
- Zu diesem Zweck werden zunächst Bedrohungen und deren Auswirkungen identifiziert.
- In weiteren Schritten werden Vorsorgemaßnahmen zur Minimierung der Risiken getroffen und Notfallpläne für die Reaktion auf Geschäftsunterbrechungen erstellt.



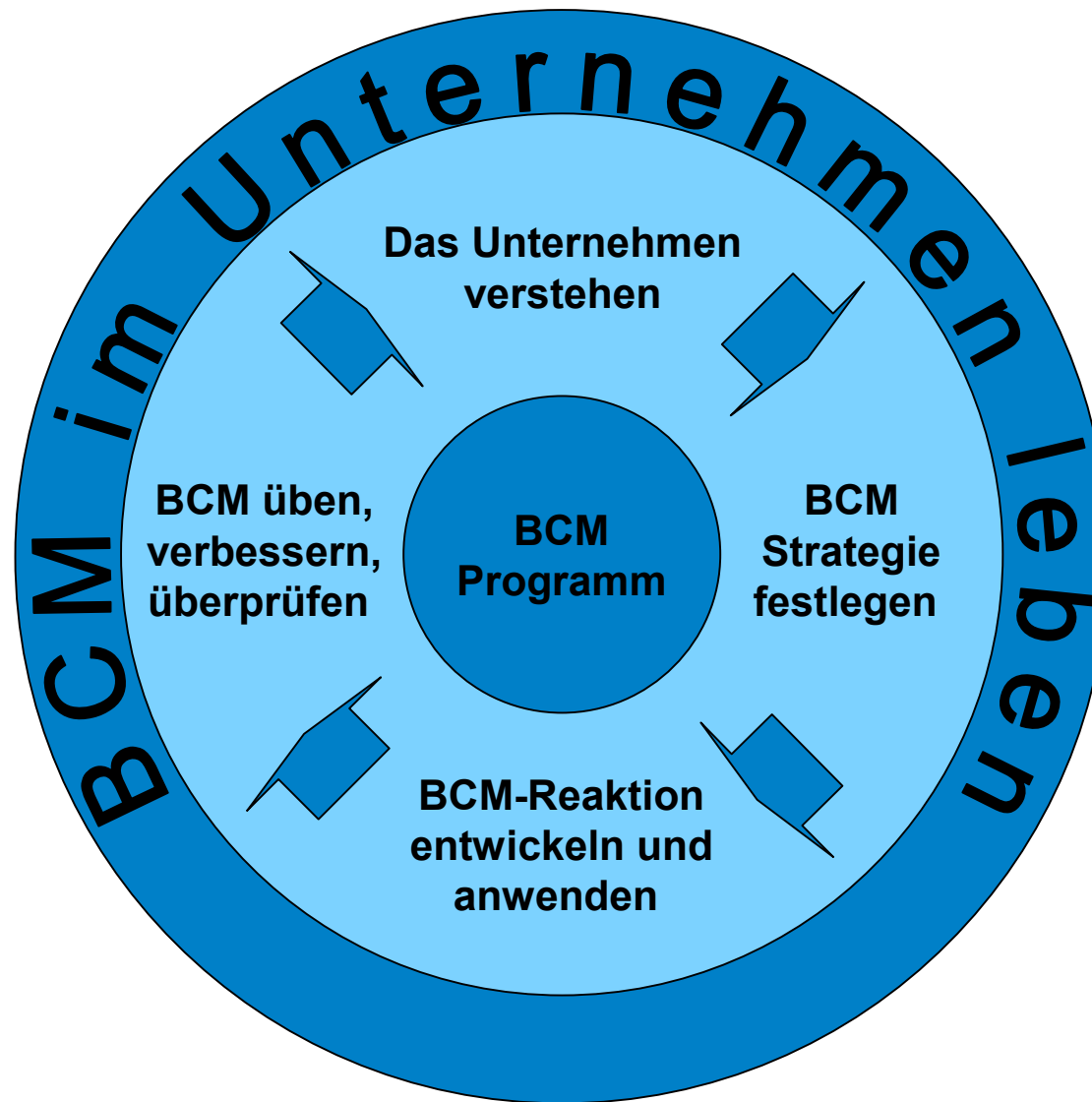
# Abgrenzung Notfall - Kommentar

Wird durch BS 25999 abgedeckt



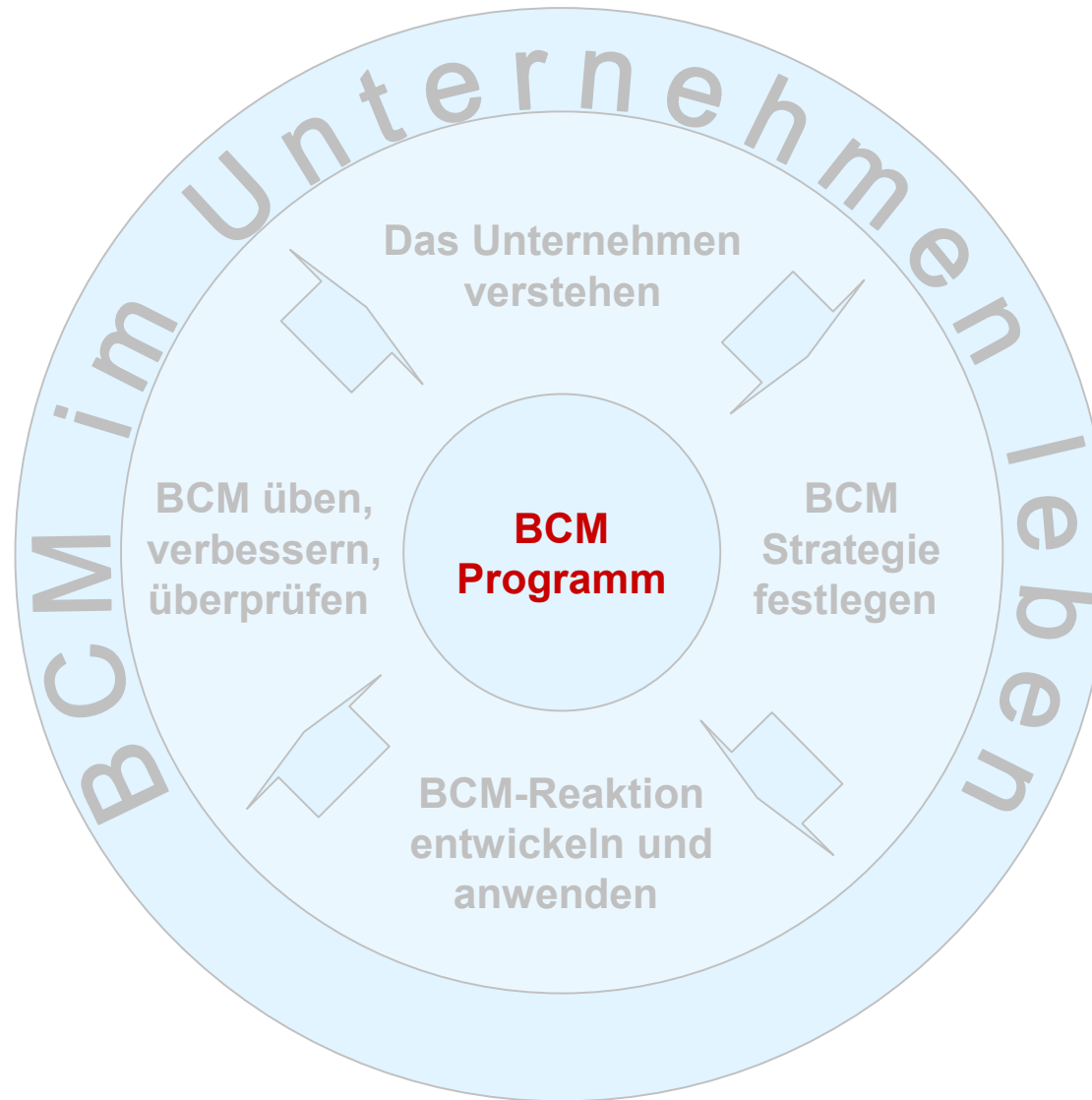


# Der BCM Kreislauf





# BCM Programm





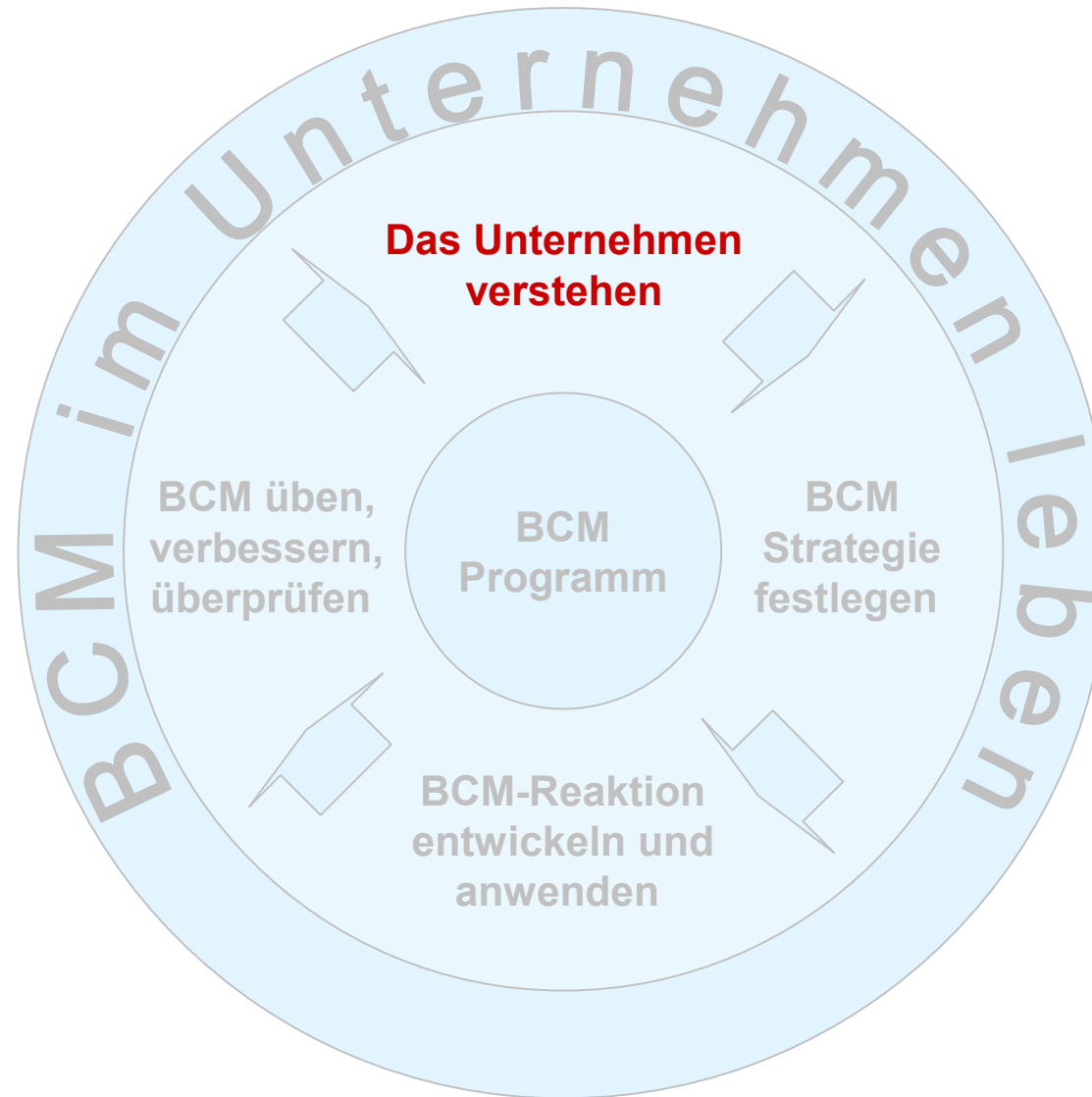
# BCM Programm

---

- Kernstück des BCM-Prozesses
- Eine Person als Verantwortlicher für die Durchführung der einzelnen Prozessbausteine im Rahmen der BCM Policy
- Ein oder mehrere Personen, die dabei unterstützen
  - in Job-Beschreibung enthalten
  - Arbeitsaufwand ist festgelegt
- Trägt BCM in das Unternehmen
- Dokumentiert alle BCM-Prozesse



# Das eigene Unternehmen verstehen





# Das eigene Unternehmen verstehen

- BIA (Business Impact Analysis)
  - Erfassen von geschäftskritischen Prozessen
  - Max. tolerierbare Ausfalldauer von Prozessen
    - Schadenserhebung als Begründung  
-> Ermittlung von geschäftskritischen Prozessen
  - Aktivitäten, Assets und Ressourcen bestimmen
- Risk-Assessment, Bedrohungsanalyse
  - Bedrohung, Gefahr
  - Schadenspotential



## Das Unternehmen verstehen - Kommentar

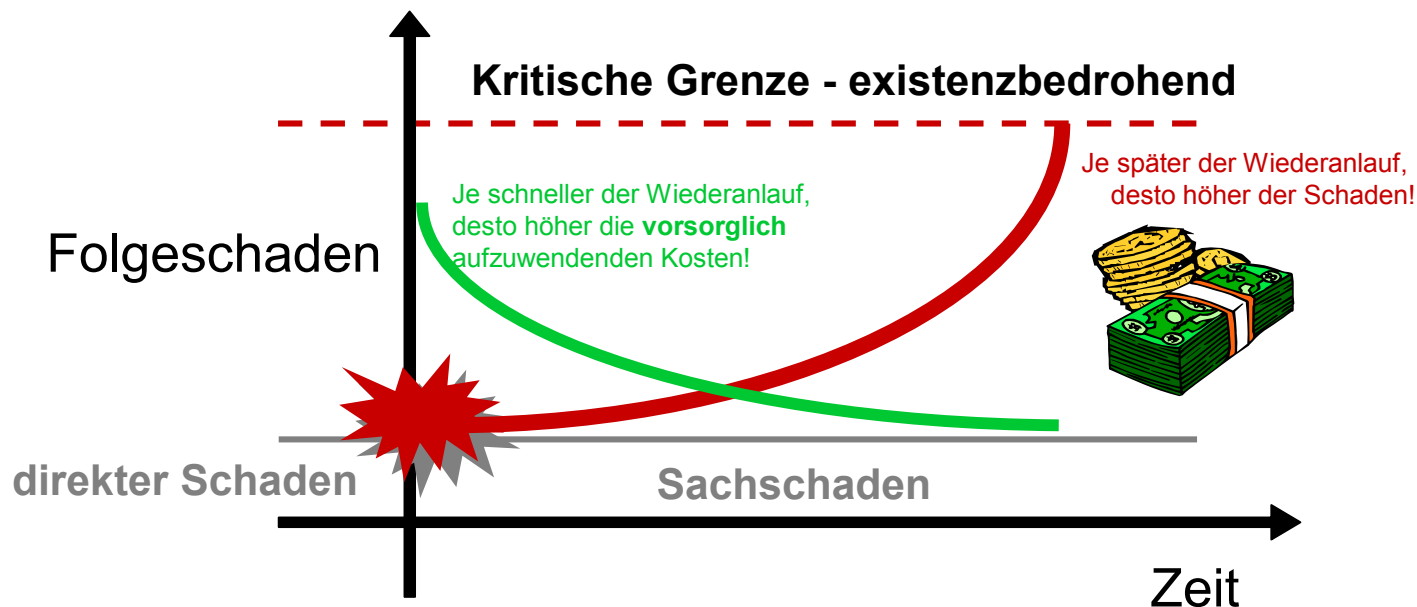
- Ermittlung der Anforderungen an IT-Anwendungen fehlt
  - Max. Ausfalldauer (RTO)
  - Max. Datenverlustzeit (RPO)
  - Ermittlung der daraus resultierenden Anforderungen an IT-Ressourcen



# Das Unternehmen verstehen - Kommentar

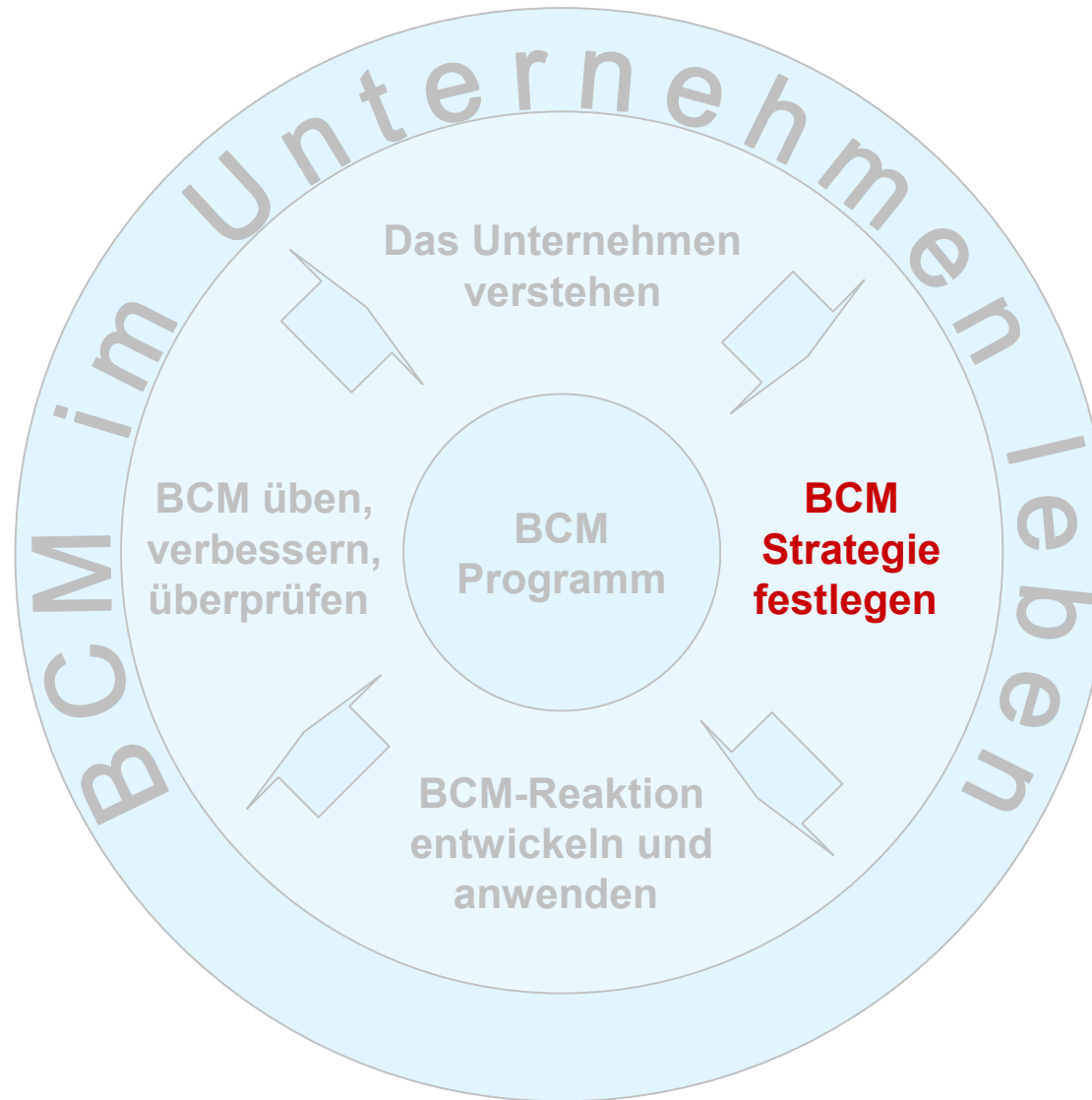
Gesamtschaden ist Summe aus

- direktem Schaden
  - wenig zeitabhängig
  - versicherbar
  - maximale Höhe - komplette Zerstörung des im Szenario betrachteten Objekts
- Folgeschaden
  - stark zeitabhängig
  - kaum versicherbar
  - realistische Höhe schwer ermittelbar





# BCM Strategie festlegen





# BCM Strategie festlegen

- Entwickeln von Strategien und Vorsorgemaßnahmen für
  - Menschen
  - Gebäude, Arbeitsplätze
  - Technologie
  - Informationen
  - Betriebsmittel (Handakten, Lagergüter etc)
  - Geschäftspartner

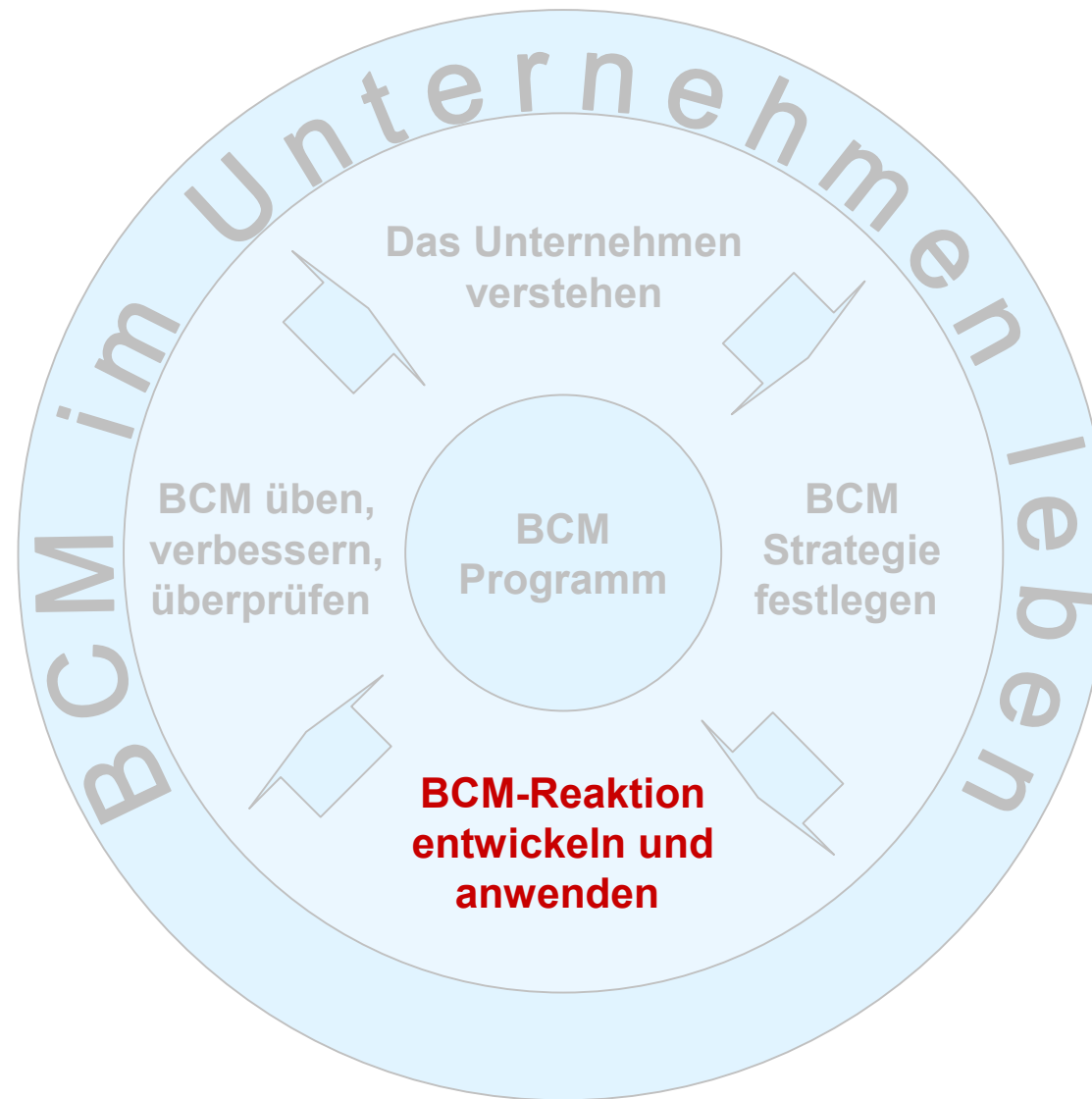


# BCM Strategie festlegen - Kommentar

- IT-Strategien fehlen
  - 2 getrennte Rechenzentrums-Standorte
  - Server redundant vorhalten
    - spiegeln
    - clustern
    - Einsatz von VM-Ware
  - Ersatz-Server vorhalten
  - Notfalllieferabkommen mit Lieferanten abschließen
  - Datensicherungen auslagern
  - Datenleitungen redundant vorhalten
  - TK-Anlage redundant vorhalten
  - ...



# BCM-Reaktion entwickeln und anwenden





# BCM-Reaktion entwickeln und anwenden

- Erstellen von Notfallplänen für
    - Incident Management Team (IMT) / Crisis Mngmt. Team (CMT)
      - Rollen einzelner Personen
      - Krisenstabsraum
      - Aktivitäten, Checklisten
      - Kontaktdaten
      - Empfehlungen für Außendarstellung im Notfall
      - Umgang mit Kapitaleignern
    - Business Continuity Plan (BCP)
      - Teams / Rollen
      - Aktivitäten, Checklisten
      - Kontaktdaten
      - Mindestressourcen
- nicht planbar
- planbar



## BCM-Reaktion entwickeln und anwenden - Kommentar

- Alarmierung und Eskalation fehlen
  - Alarmierungslisten
  - Eskalations- / Entscheidungspfade
- IT-Notfallplan fehlen
  - Notwendige IT-Ressourcen
  - IT-Wiederaanlaufpläne (Aktivitäten, Checklisten)
  - Kontaktdaten



# consequa Gliederungsvorschlag für Business Continuity Plan

1	Einleitung	4.3.1	Ersatzverfahren
1.1	Vorwort zum BC-Plan	4.3.2	Abweichungen gegenüber dem Normalbetrieb
1.2	Änderungsnachweis	4.3.3	Zusätzliche Tätigkeiten im Notbetrieb
1.3	Abkürzungsverzeichnis	4.4	Für den Notbetrieb benötigte Dokumente und Formulare
1.4	Pflege- und Änderungsdienst	5	Zusatzinformationen
1.5	Mitgeltende Dokumente	5.1	Anfahrtspläne
2	Notfallorganisation	5.2	....
2.1	Notfallteams	6	Adress- und Telefon-Verzeichnisse
2.2	Änderung der Kompetenzen	6.1	Mitarbeiterliste
3	Alarmierung / Eskalationsverfahren	6.2	Standorte
4	Wiederanlauf der Geschäftsfunktionen (je Notfallteam ein Kapitel)	6.3	Dienstleister
4.1	Ausweichstandorte	7	Wiederanlaufziele und Ressourcen
4.2	Erste Aktivitäten am Ausweicharbeitsplatz	7.1	Allgemeine Beschreibung der Wiederanlaufstrategie
4.3	Notbetrieb	7.2	Wiederanlaufklassen
		7.3	Mindestressourcen

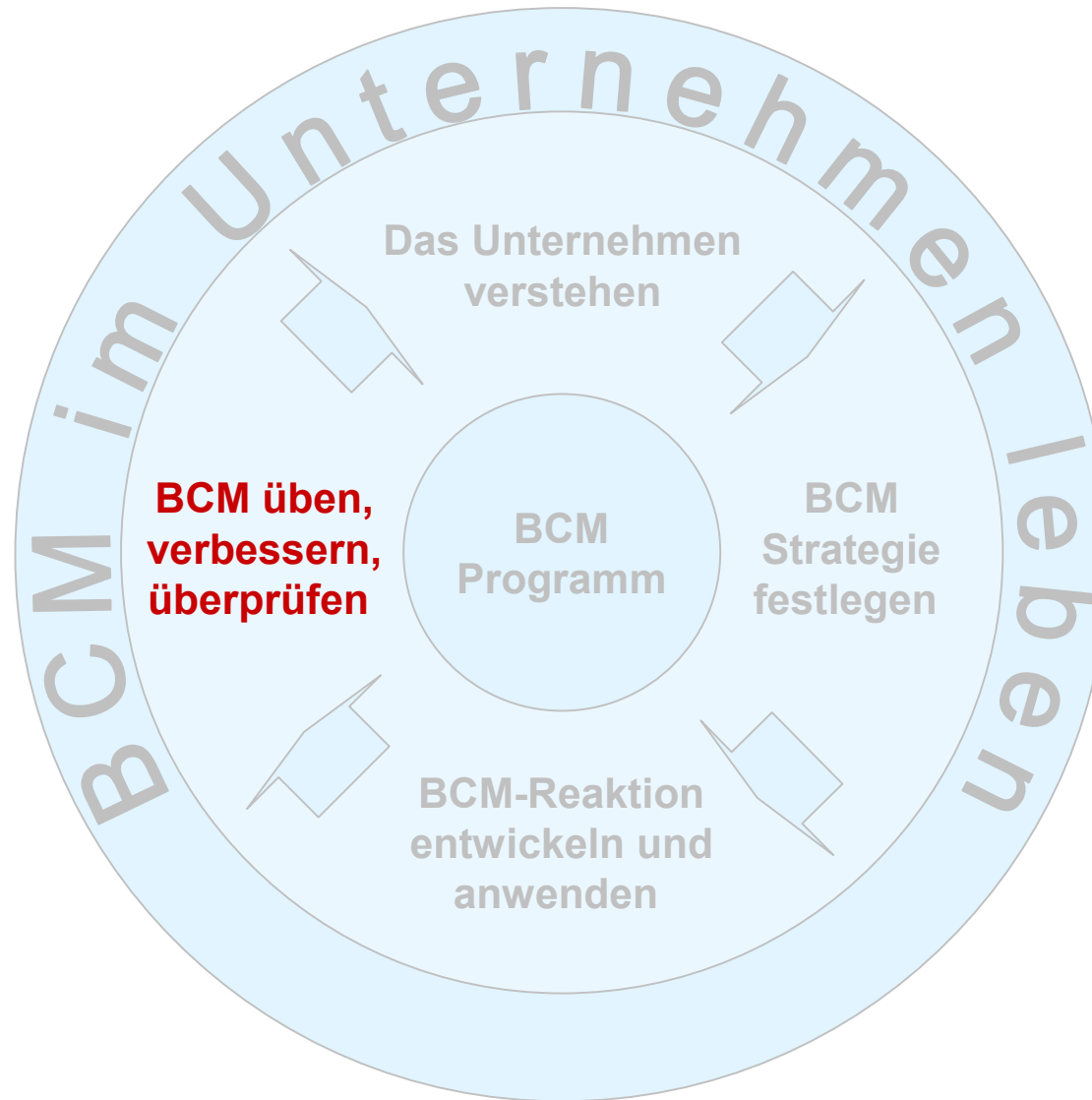


# consequa Gliederungsvorschlag für IT-Notfallplan

1	Einleitung	4.3	Rekonstruktion Hardware
1.1	Vorwort zum IT-Plan	4.4	Rekonstruktion Betriebssystem
1.2	Änderungsnachweis	4.5	Datenrücksicherung
1.3	Abkürzungsverzeichnis	4.6	Anwendungsfreigabe
1.4	Pflege- und Änderungsdienst		
1.5	Mitgeltende Dokumente	5	Zusatzinformationen
		5.1	Anfahrtspläne
		5.2	....
2	Notfallorganisation		
2.1	Notfallteams	6	Adress- und Telefon-Verzeichnisse
2.2	Änderung der Kompetenzen	6.1	Mitarbeiterliste
		6.2	Standorte
3	Alarmierung / Eskalationsverfahren	6.3	Dienstleister
4	Masterplan des Wiederanlaufs (Übersicht über die gesamte IT)	7	Wiederanlaufziele und Ressourcen
4.1	Wiederanlauf der Infrastruktur (je Notfallteam ein Kapitel)	7.1	Allgemeine Beschreibung der Wiederanlaufstrategie
4.2	Ausweichstandorte	7.2	Wiederanlaufklassen
		7.3	Konfigurationen



# BCM Üben, verbessern, überprüfen



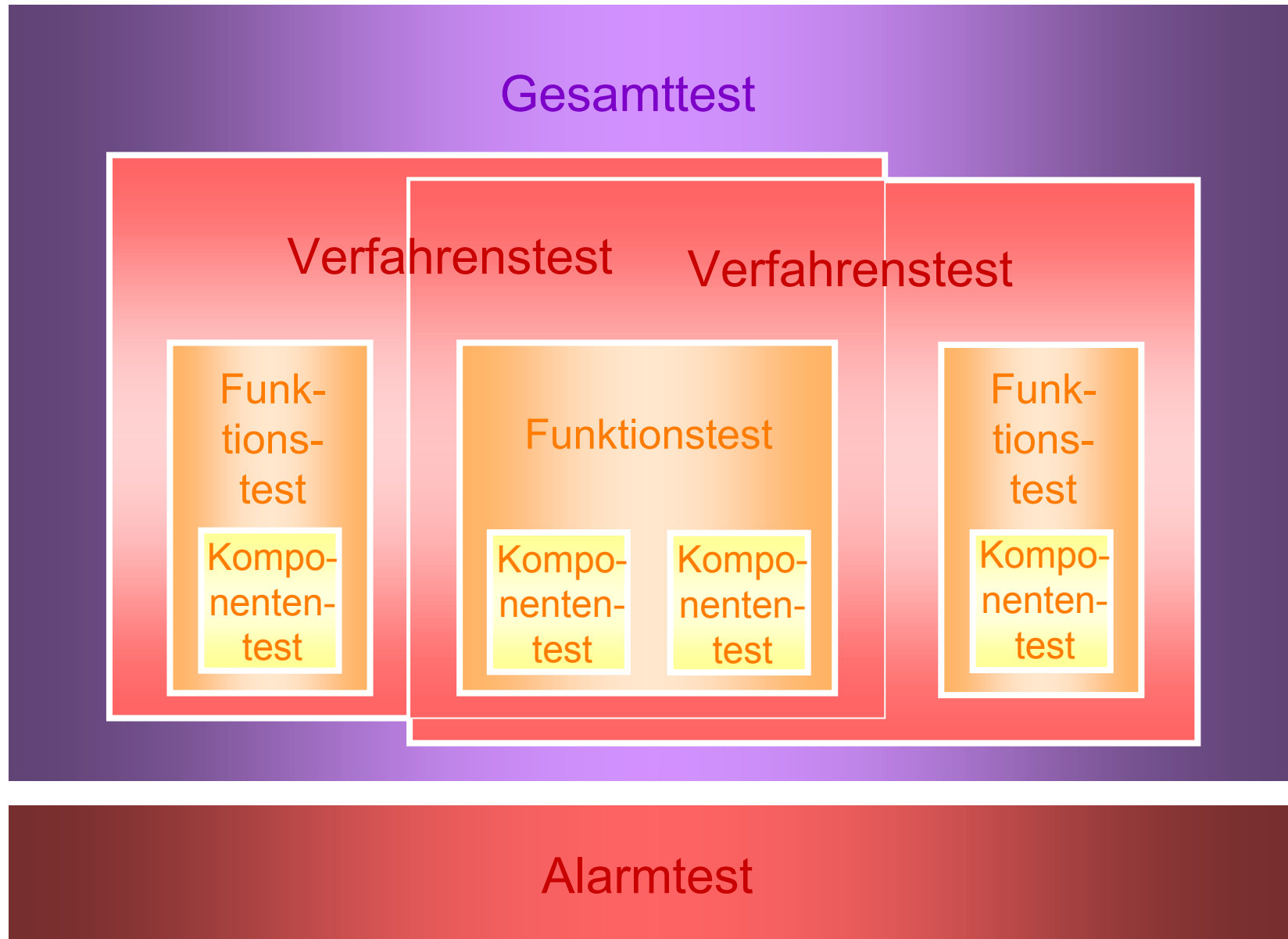


## BCM Üben, verbessern, überprüfen

- Alle Vorsorgemaßnahmen und Notfallpläne müssen durch geeignete Übungen überprüft werden
- Die Übungen sollten realitätsnah sein und sich an die vorher diskutierten Notfallszenarien halten
- Die Ergebnisse sollten wieder in die Vorsorgemaßnahmen einfließen
  - Ist die Vorsorge ausreichend?
  - Wird die vorgegebene Zeit eingehalten?
  - Wird das Ziel erreicht?
- Diese Übungen sind in regelmäßigen Abständen durchzuführen, um Veränderungen im Unternehmen mit abzudecken

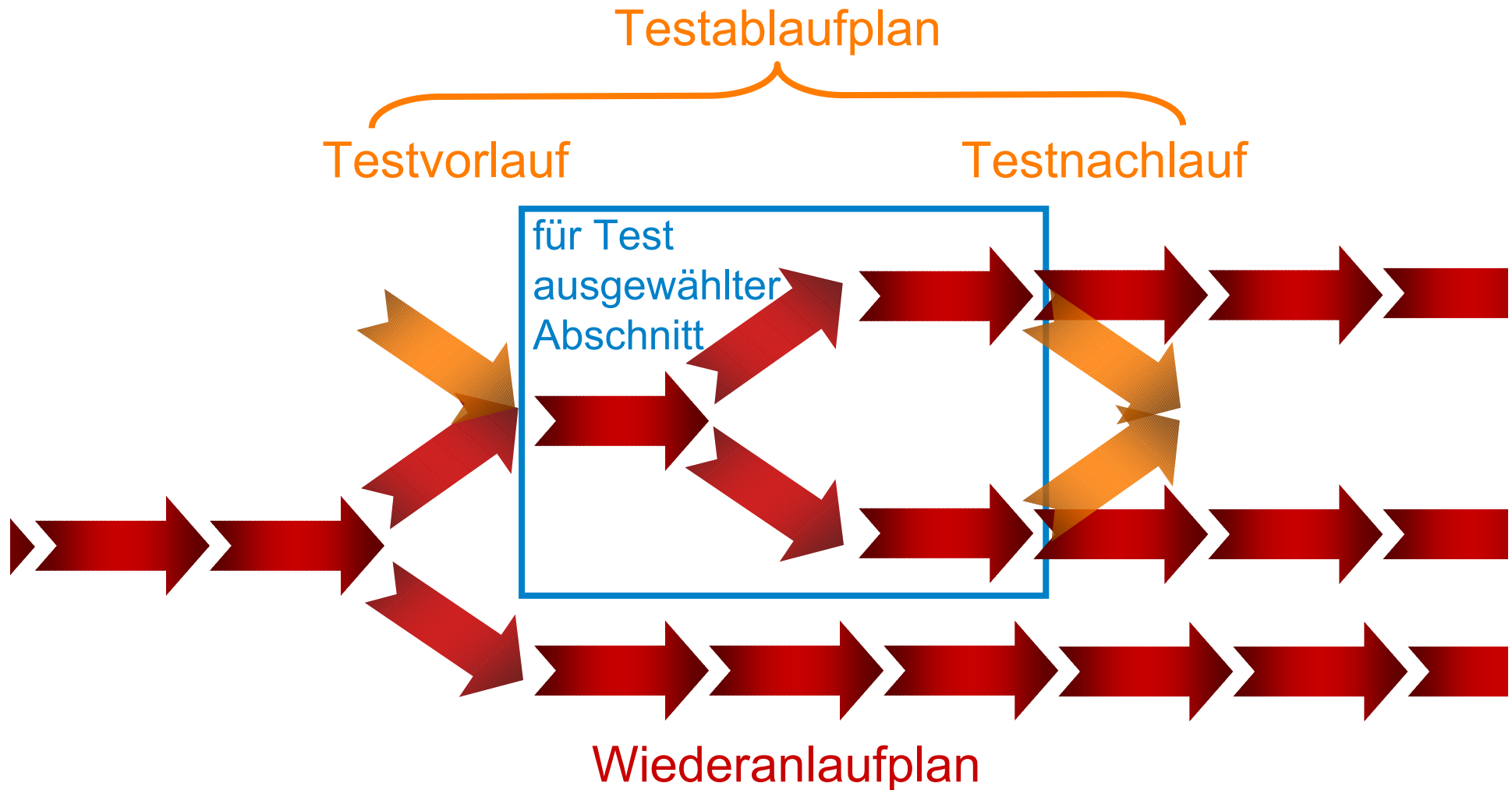


# Beispiel: consequa-Teststufen



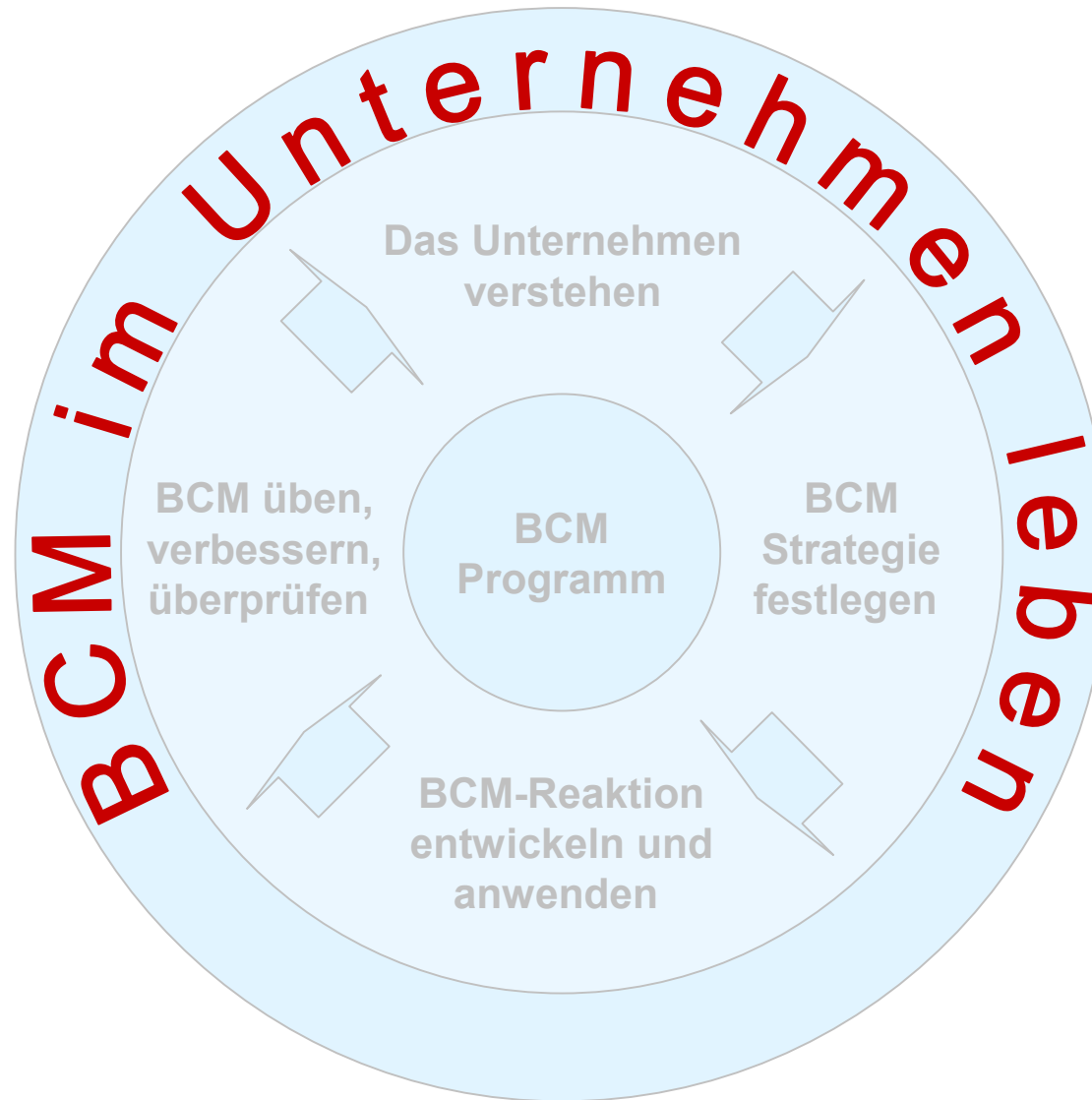


# Testablauf





# BCM im Unternehmen leben





## BCM im Unternehmen leben

---

- Im Unternehmen ist für alle Phasen des BCM-Programms hohe Transparenz zu schaffen
- Das Bewusstsein (Awareness) über die BCM-Kultur im Unternehmen muss gefördert werden
  - z. B. durch regelmäßige Trainings und Übungen aller beteiligten Personen



# BCM im Unternehmen leben - Kommentar

---

- Binnenmarketing
- Beteiligung des Vorstands / Geschäftsführung
- Change Management muss BCM beinhalten



# Was kommt im Standard BS 25999-2:2007



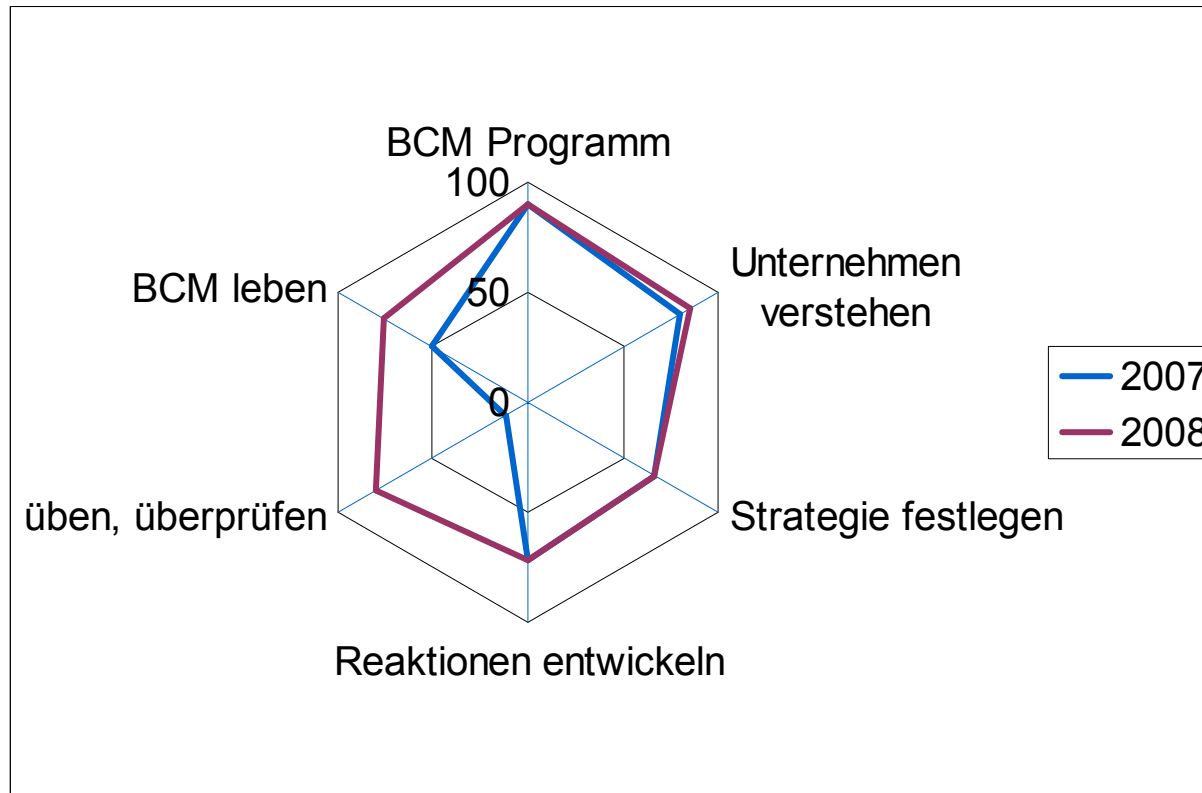


## Was kommt im Standard BS 25999-2:2007

- BS 25999-2:2007 beschreibt den Prozess, um eine Zertifizierung für die Business Continuity-Fähigkeit zu erreichen, die der Unternehmensgröße und –Komplexität angemessen ist.
  - Wird voraussichtlich dem Audit-Verfahren aus PAS56 ähnlich sein
  - Erscheint Anfang 2007
- Die einzelnen Bestandteile des BCM-Programms werden durch einen einheitlichen Fragenkatalog auf ihren Erfüllungsgrad hin untersucht.
- Der Fragenkatalog ist standardisiert, dadurch sind die Ergebnisse vergleichbar
  - mit den Ergebnissen aus vorangegangenen Audits
  - mit den Ergebnissen einzelner Unternehmensbestandteile
  - mit den Ergebnissen anderer Unternehmen

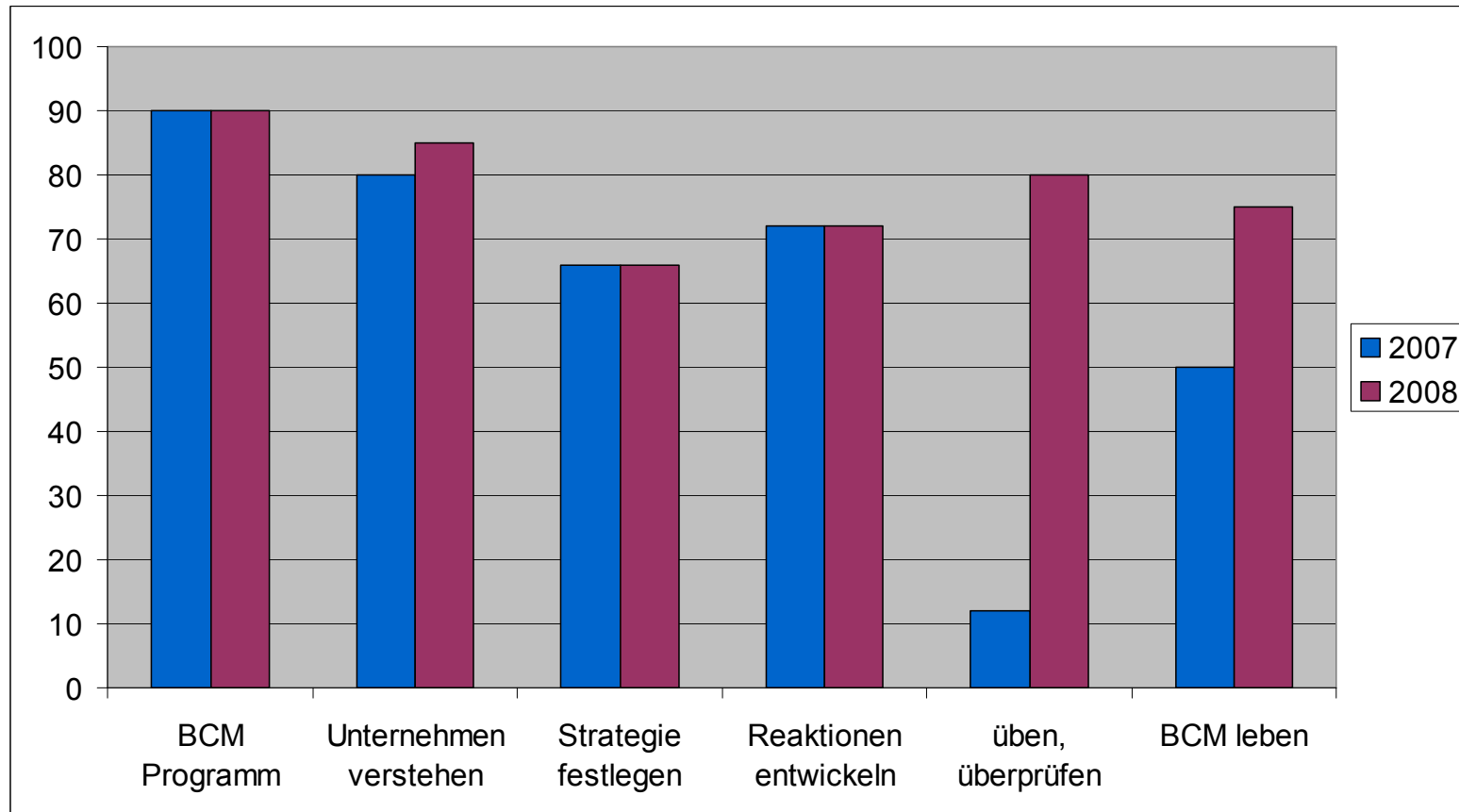


# Mögliches Ergebnis eines Audits





# Mögliches Ergebnis eines Audits



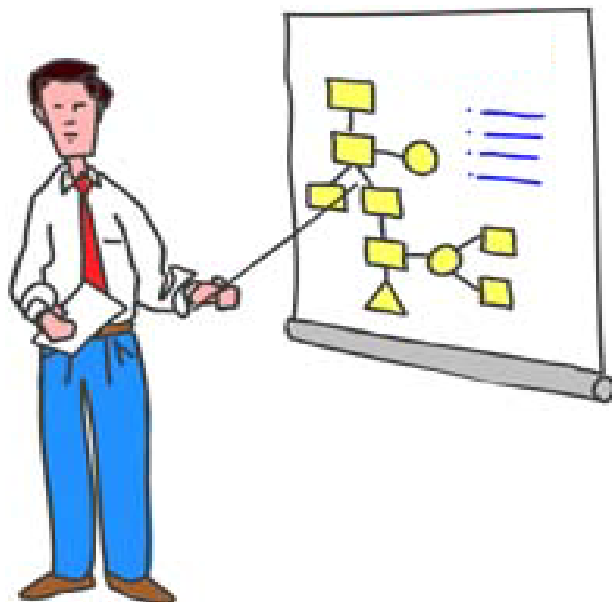


# BS 25999 - Resumée

- **Positiv**
  - Standard für BCM erstmalig formuliert
  - Aus der Praxis
  - In sich abgeschlossene Methode
- **Kritik**
  - IT zu wenig berücksichtigt
  - Fehlende Abgrenzung gegenüber IT-Security, Risikomanagement
  - Keine weiterführenden Materialien
  - Durchführung ist aufwendig



# Vielen Dank für Ihre Aufmerksamkeit!



Dipl.-Ing.

**Tobias Timmler**

Berater

consequa GmbH  
Süderstraße 73  
20097 Hamburg  
[www.consequa.de](http://www.consequa.de)

Tel.: 040 / 78 89 70 64  
Fax: 040 / 78 89 70 66

[tobias.timmler@consequa.de](mailto:tobias.timmler@consequa.de)