



Konkretes Vorgehen in einem BCM-Projekt

**CAST-Workshop
Darmstadt 21.02.2008**

Bernd Ewert





- Unternehmensstandort Hamburg
- gegründet 1.4. 2005
- langjährige Beratungserfahrungen
 - Business Continuity / IT-Recovery
 - Information Security / IT-Sicherheit
 - Service Quality / SLAs und Regeln
- 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.





Regelwerke, in denen BCM gefordert wird

- IDW RS FAIT 1 September 2002
- IDW RS FAIT 2 September 2003
- IDW RS FAIT 3 Juli 2006
- BaFin MaRisk Dezember 2005
- CobiT aktuell 4.0: Mai 2007
- ITIL aktuell V.3: Juni 2007
- ISO/IEC 20000 Dezember 2005
- ISO/IEC 27002 als 17799: Juni 2005
- ISO/IEC 27001 Oktober 2005
- BS 25999-1 November 2006
- BS 25999-2 November 2007
- BSI-Standard 100-4 geplant für 2008

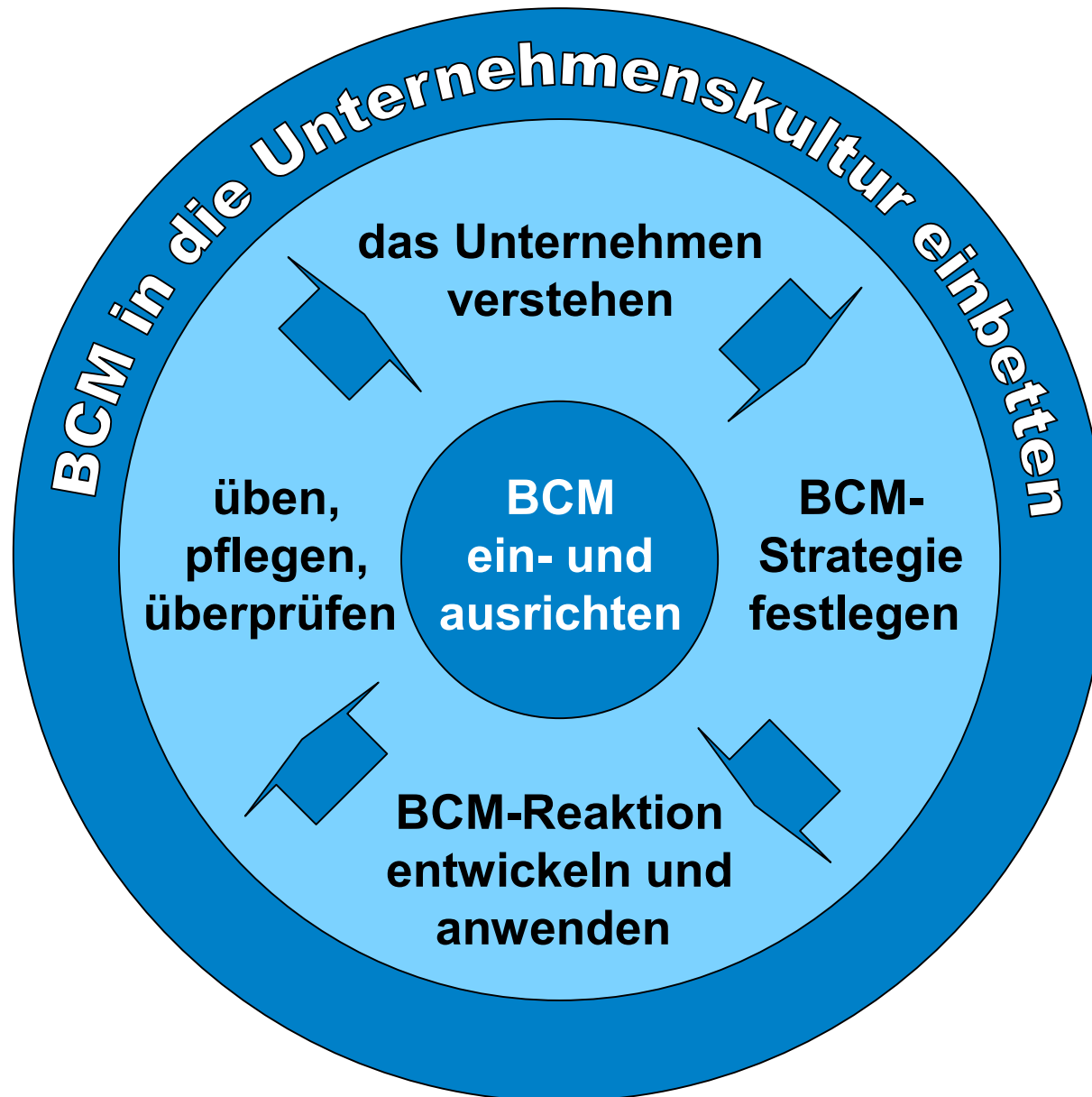


BCM und Nachbardisziplinen

- **Business Continuity**
 - sichert die angemessene Verfügbarkeit und Wiederherstellung **kritischer Ressourcen**, die zur Ausübung kritischer Geschäftsfunktionen benötigt werden
- **Information Security**
 - sichert angemessene Verfügbarkeit, Vertraulichkeit, Integrität, Verbindlichkeit der genutzten **Informationen**
- **Arbeitssicherheit**
 - sichert das **Personal** gegen Gefahren bei der Arbeit ab
- **Überschneidungen**
 - Verfügbarkeit von **Personal** und **Informationen**
 - Verfügbarkeit von **Informationstechnik**
 - **Sofortmaßnahmen im Notfall** und **Notfallvorsorge für IT**



BCM nach BS 25999-1





„den Rahmen für BCM schaffen“

- Projekt mit Verantwortung bei Unternehmensleitung
- grundsätzliche Einordnung
 - keine eigene Leitlinie => Sicherheitsleitlinie
 - Regelkreise koppeln mit anderen Zyklen
- Abgrenzung Krisen- und Notfallmanagement





„das Unternehmen verstehen“

- Ziele, Prozesse, Ressourcen aufnehmen
- Schäden durch Ausfälle bestimmen
- kritische Abläufe finden
- Ressourcen zu Abläufen zuordnen
- Bedrohungen analysieren

noch nicht:

- Maßnahmen identifizieren





Wie entsteht Kontinuität?

Geschäftsfunktionen

haben

Aufgaben

werden bearbeitet durch

Arbeitsmittel

nutzen

Menschen

nutzen

Dienstleistungen

befinden sich an

Standorte

werden erbracht von

Fremdfirmen

oder

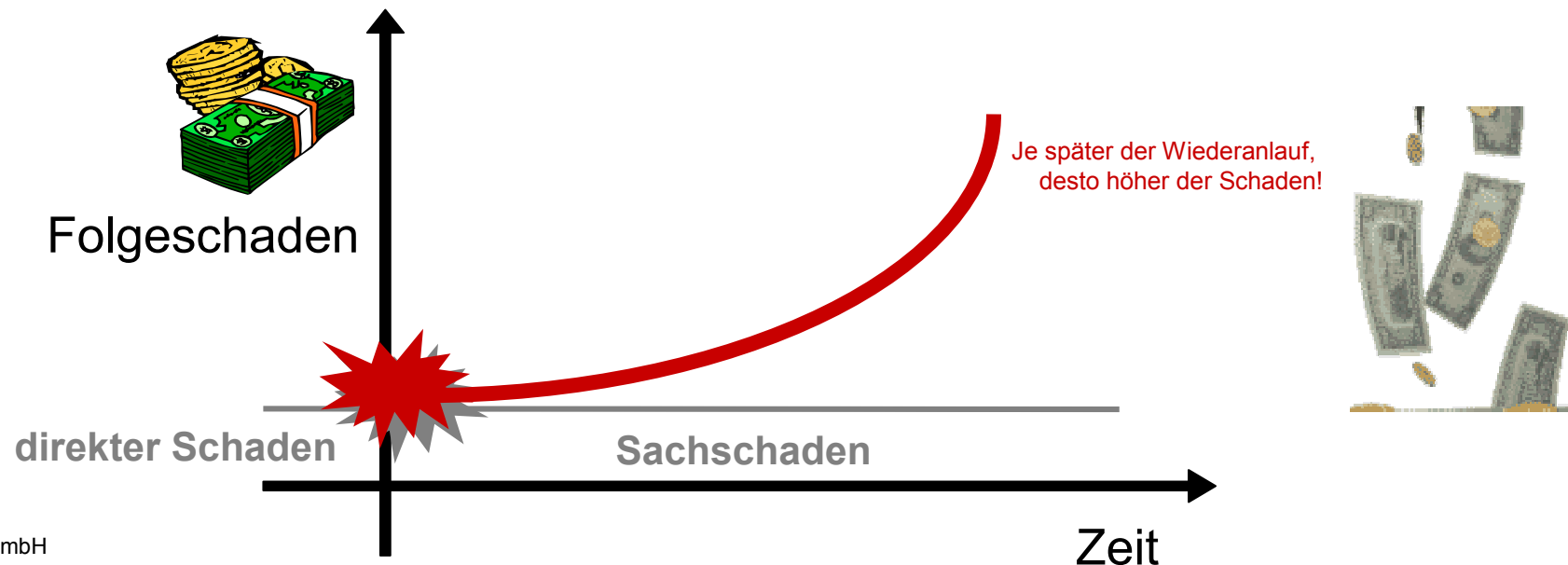
Geschäftsfunktionen



Business Impact Analyse (BIA)

Gesamtschaden ist Summe aus

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





Beispiele für Schadensklassen

- monetär

Nr.	Schadensfaktor	Schadensklassen				
		unbedeutend	spürbar	erheblich	schwerwiegend	existenzbedrohend
M1.	Opportunitätskosten	kein in der Bilanzsumme / im Gewinn / im Umsatz spürbarer finanzieller Schaden	unterhalb von 3% der Bilanzsumme / des Gewinns / des Umsatzes	zwischen 3% und 10% der Bilanzsumme / des Gewinns / des Umsatzes	zwischen 10% und 30% der Bilanzsumme / des Gewinns / des Umsatzes	größer als 30% der Bilanzsumme / des Gewinns / des Umsatzes
M2.	entgangene Gewinne					
M3.	Regress- / Schadensersatzforderungen					

- qualitativ

Nr.	Schadensfaktor	Schadensklassen				
		unbedeutend	spürbar	erheblich	schwerwiegend	existenzbedrohend
Q1.	Verlust von Aufträgen bzw. Kunden	keine merklichen Verluste	vereinzelte oder nur kurzfristige Verluste	spürbare Verluste von Kunden und / oder Aufträgen über längeren Zeitraum	deutliche Verluste von Kunden und / oder Aufträge über längeren Zeitraum	nachhaltige Einbuße eines beträchtlichen Teils der Kunden und / oder Aufträge
Q2.	Image- / Vertrauensverlust (Außenwirkung)	keine oder kaum wahrnehmbar negative Außenwirkung	wahrnehmbare negative Außenwirkung von kurzfristiger Dauer	deutlich wahrnehmbare negative Außenwirkung über einen längeren Zeitraum	breite und lang anhaltende negative Außenwirkung, die sich auch in Massenmedien wieder spiegelt	lang anhaltende desaströse Außenwirkung



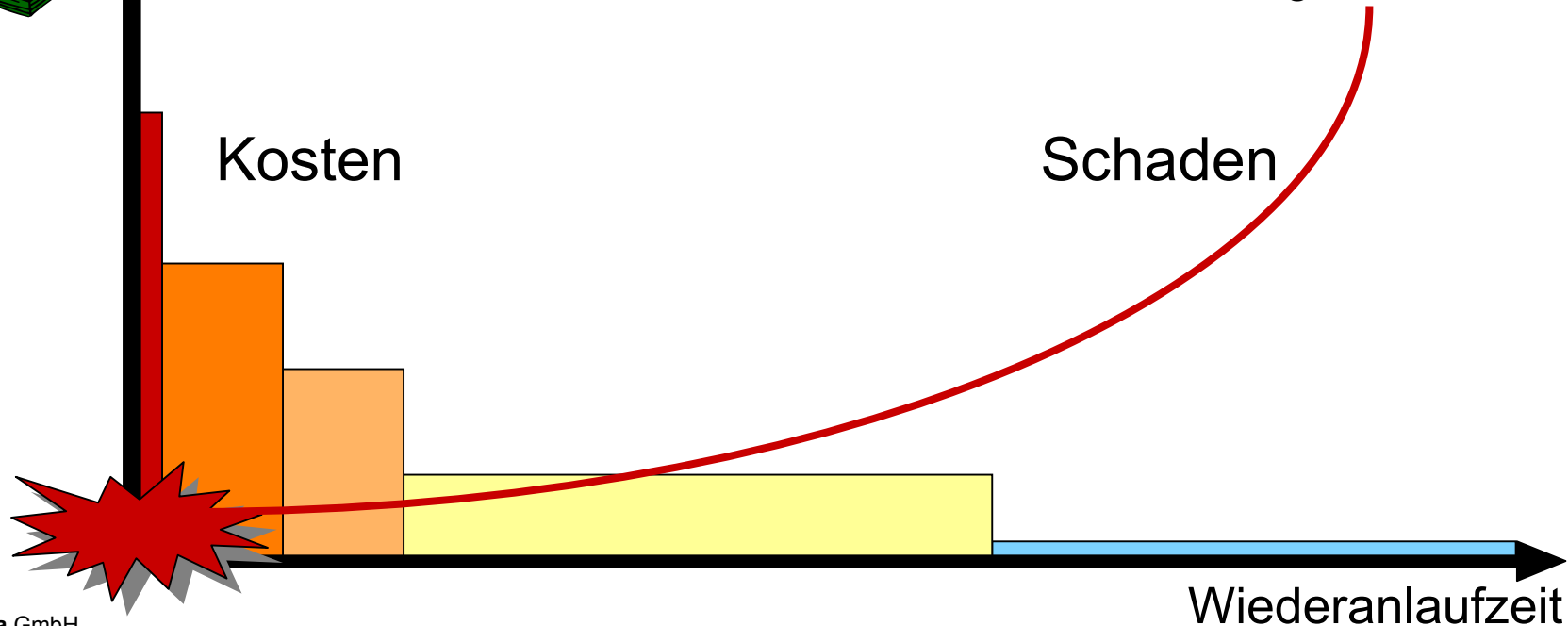
Beispiele für Wiederanlaufklassen

z.B.

WAK	Bewertung	Wiederanlaufzeit
1	extrem zeitkritisch	4 Stunden
2	sehr zeitkritisch	24 Stunden
3	zeitkritisch	48 Stunden
4	weniger zeitkritisch	7 Tage
5	nicht zeitkritisch	keine Festlegung



bei IT zusätzlich Datenverlust berücksichtigen





Welche Ausfälle werden fokussiert?

Katastrophe

- großflächige Zerstörungen oder Verseuchungen
- Epidemien



Notfall

- **Ausfall eines Gebäudes mit zentralen Funktionseinheiten**
- **Ausfall eines Rechenzentrums**



Störung

- Ausfall eines Servers
- Ausfall eines Arbeitsplatzes



„BCM-Strategie festlegen“

- BC-Strategie bestimmen
- **jetzt:** Maßnahmen identifizieren
- Außenwelt kontaktieren
- Management zustimmen lassen





Komponenten der Wiederanlaufstrategie I

Komponenten		
Ausweichstandorte	<ul style="list-style-type: none">• eigene Standorte• Fremdstandorte	
Betriebsanlagen	<ul style="list-style-type: none">• Werke und Fabrikate• Läger und Transportmittel• Roh- und Hilfsstoffe	
Büroarbeitsplätze	<ul style="list-style-type: none">• Gebäude und Räume• Arbeitsmittel (PC usw.)	
Akten und Unterlagen	<ul style="list-style-type: none">• elektronisches Archiv• Duplikate	
externe Unternehmen	<ul style="list-style-type: none">• Lieferanten• Partner• Dienstleister• Kunden	



Komponenten der Wiederanlaufstrategie II

Komponenten		
zentrale IT-Services	<ul style="list-style-type: none">• Ausweichstandorte• IT-Systeme	
Datensicherung	<ul style="list-style-type: none">• Datensicherung• Auslagerung• Datenwiederherstellung	
Datenkommunikation	<ul style="list-style-type: none">• Netzumschaltung auf Ausweichstandorte	
Sprachkommunikation	<ul style="list-style-type: none">• Netzumschaltung auf Ausweichstandorte	



„BCM-Reaktion entwickeln und anwenden“

- Organisationsstruktur für Reaktion aufbauen
- Notfallpläne erstellen

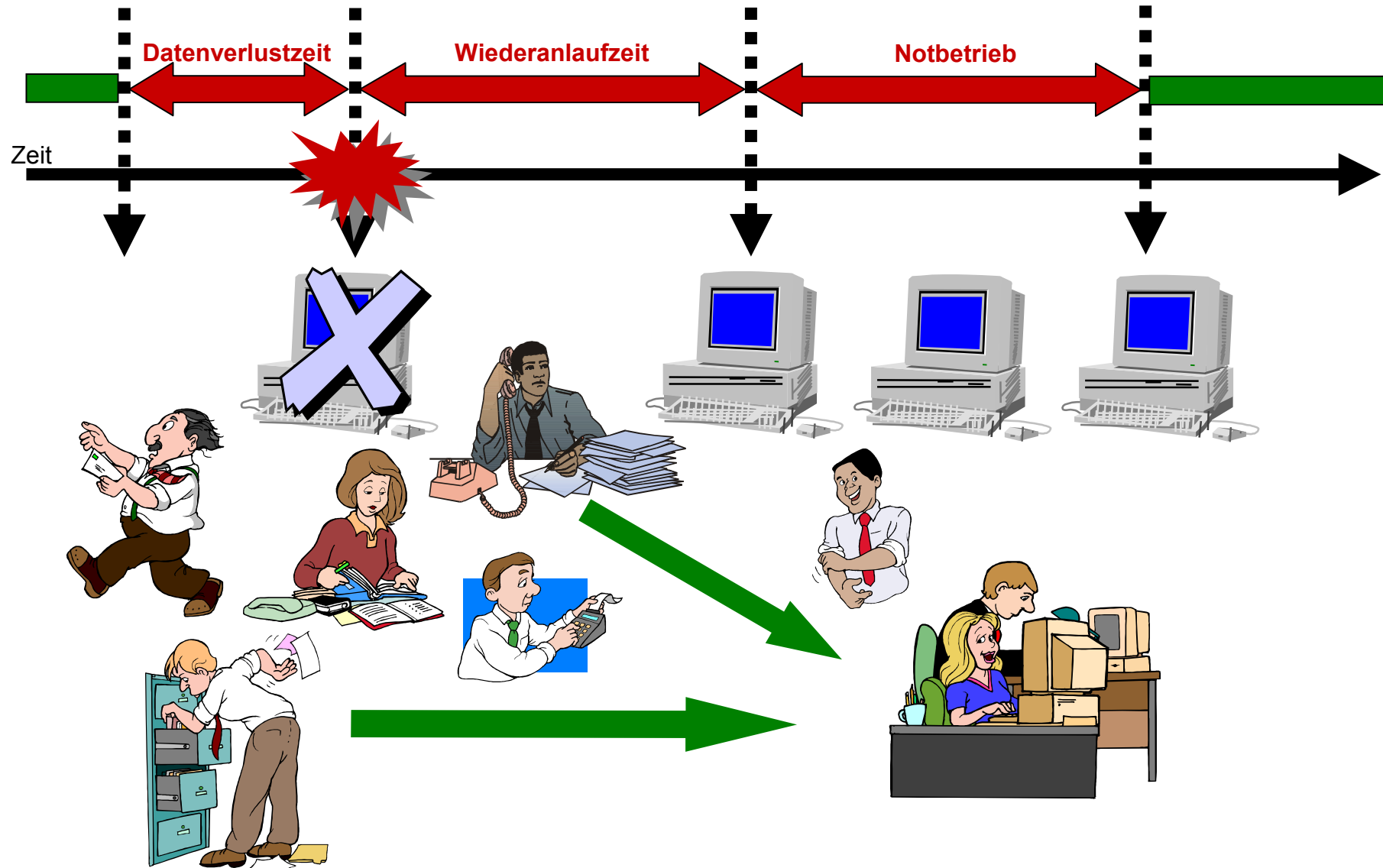
vor allem aber:

- Voraussetzungen schaffen
 - Ausweichstandorte einrichten
 - Verträge mit Dienstleistern schließen
 - technische Lösungen umsetzen




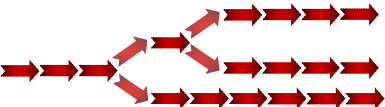



Geschäftsfortführung und Wiederanlauf



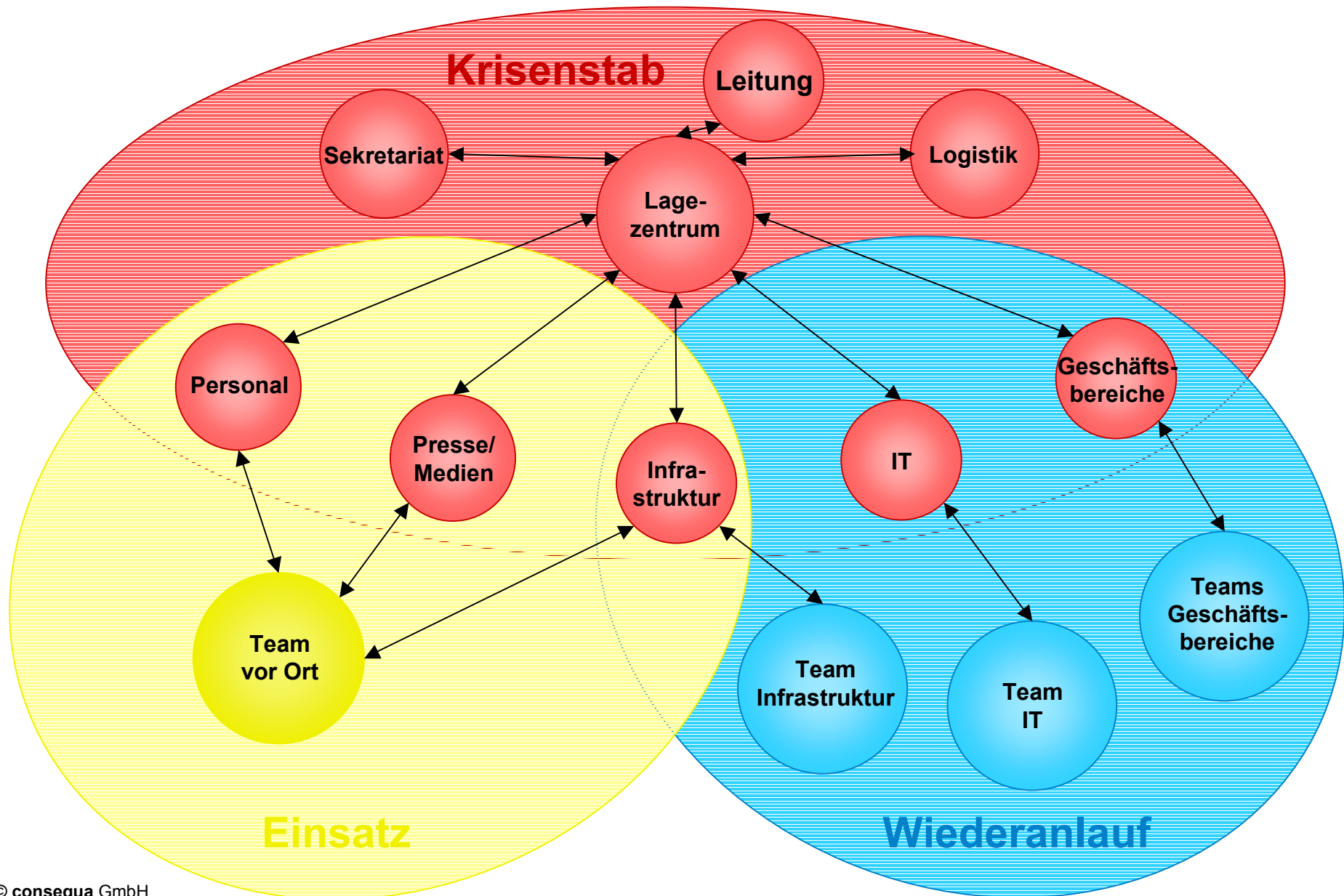


Komponenten der Reaktion

Komponenten	
Notfallorganisation	<ul style="list-style-type: none">• Krisenstab• Notfallteam(s)• Kommunikationswege 
Verfahren zur Reaktion	<ul style="list-style-type: none">• Alarmverfahren• Sofortmaßnahmen• Überbrückungsverfahren• Wiederanlaufverfahren• Krisenmanagement 
Dokumentation (Pläne)	<ul style="list-style-type: none">• Notfallorganisation• Verfahren zur Reaktion• Kontaktverzeichnisse• Ressourcenübersichten 



Krisenmanagement





„üben, pflegen, überprüfen“

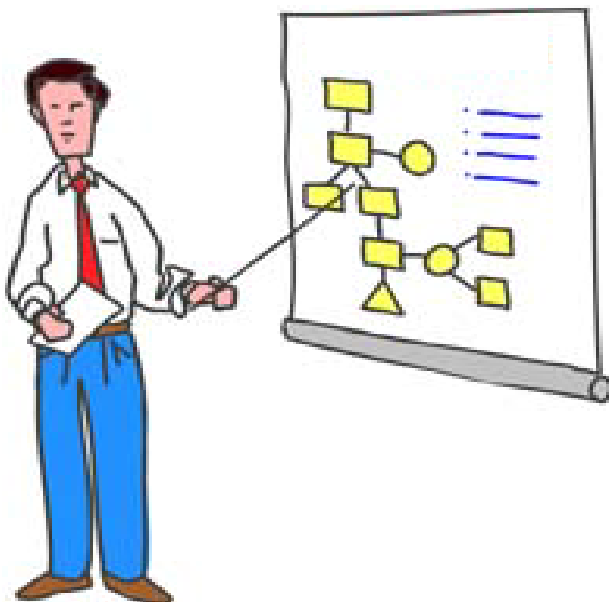
- regelmäßige BIA
- betriebliche Änderungen verfolgen
- Übungen und Tests planen und durchführen

- => Pläne überprüfen und aktualisieren





Vielen Dank für Ihre Aufmerksamkeit!



Dipl.-Inform.
Bernd Ewert
Geschäftsführer

consequa GmbH
Süderstraße 73
20097 Hamburg
www.consequa.de

Tel.: 040 / 78 89 70 61
Fax: 040 / 78 89 70 66

bernd.ewert@consequa.de