Im Notfall Business Continuity-Management

Schnittstellen und Unterschiede zwischen
Business Continuity- und Risiko-Management

SWISS GRC

SWISS GRC DAY 2018

Zürich, 29. Oktober 2018

Referent

Albert Andrist

- Certified Lead Auditor BS25999
  Business Continuity Management Systems
- Certified Security Manager CFPA
- Integraler Sicherheitsmanager SAQ
- Certified Business Risk-Manager
- Certified IT-Manager

- Langjähriger Leiter Business Continuity & Security der Gruppe Mobiliar.

- Leiter der SVV-Arbeitsgruppe zur Erstellung der BCM-Selbstregulierung für Versicherungsgesellschaften in der Schweiz im Auftrag der FINMA.

Um was geht es?

- Haben Sie ein Business Continuity Management System (BCMS) implementiert?

- Haben Sie einen Business Continuity-Plan im Falle von Cyber-Angriffen auf Ihr Unternehmen?

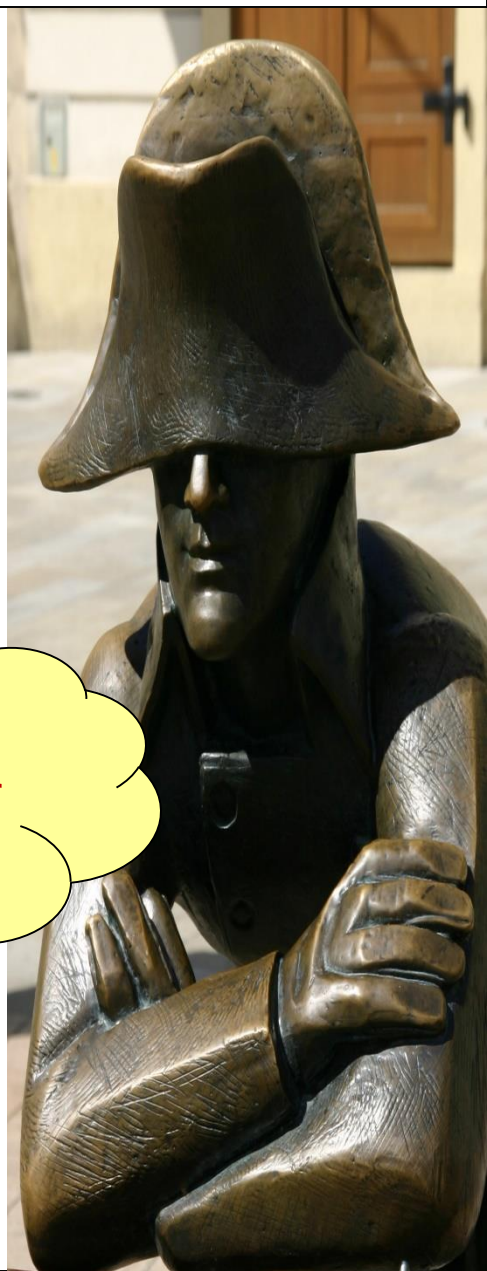
  Was tun Sie, wenn der Verwaltungsrat, die Geschäftsleitung oder die Revisoren mit dieser Frage zu Ihnen kommen?

Vorbereitet sein für den Notfall

Viele Firmen verfügen über …

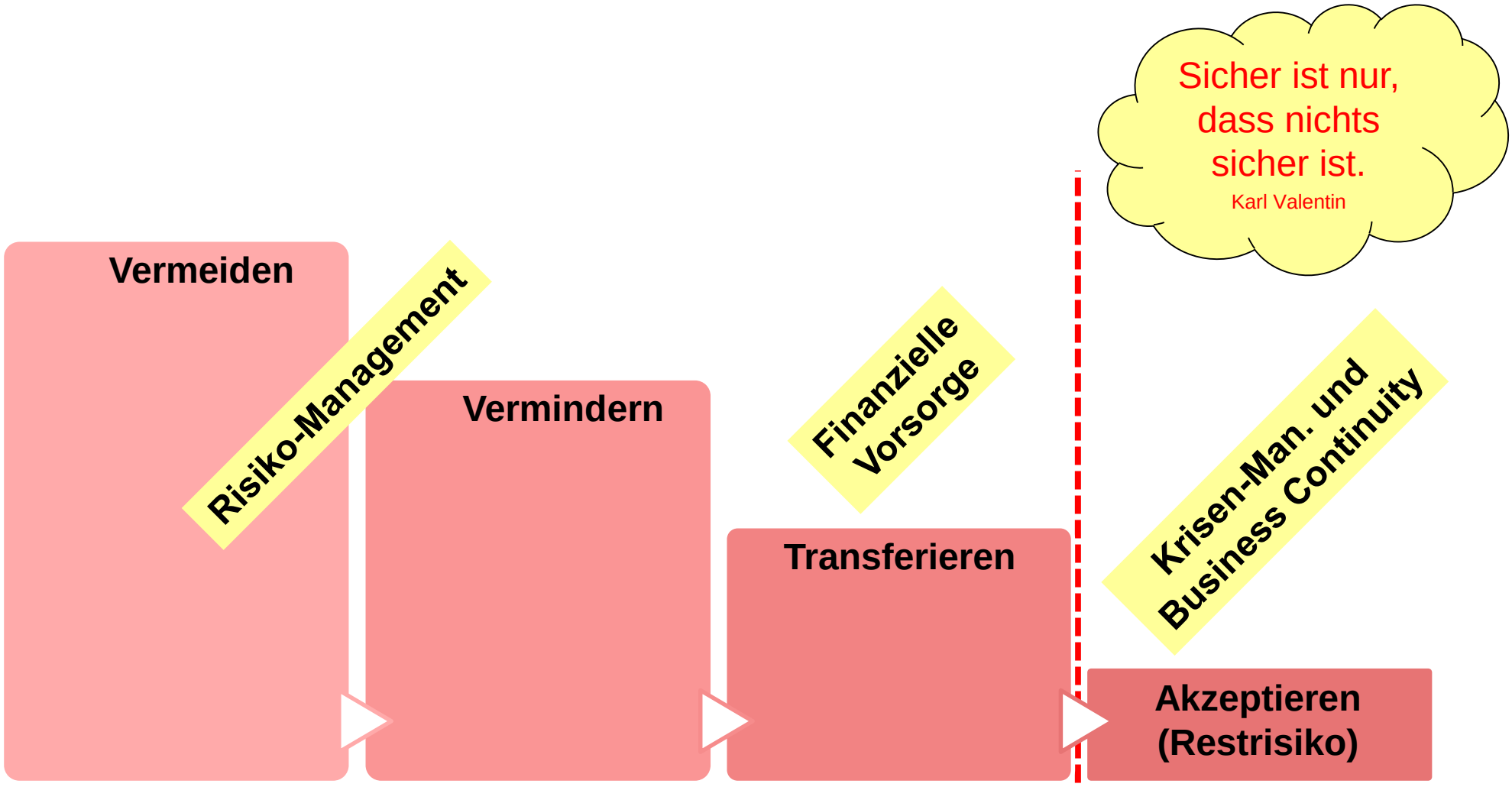
- … ein gut funktionierendes IKS und Compliance
- … ein solides Risiko-Management
- … eine kompetente Geschäftsleitung
- … einen führungsstarken CEO
- … ein abgenommenes Notfallkonzept

‚Das Glück bevorzugt den, der vorbereitet ist.‘
Louis Pasteur



Was fehlt denn noch?

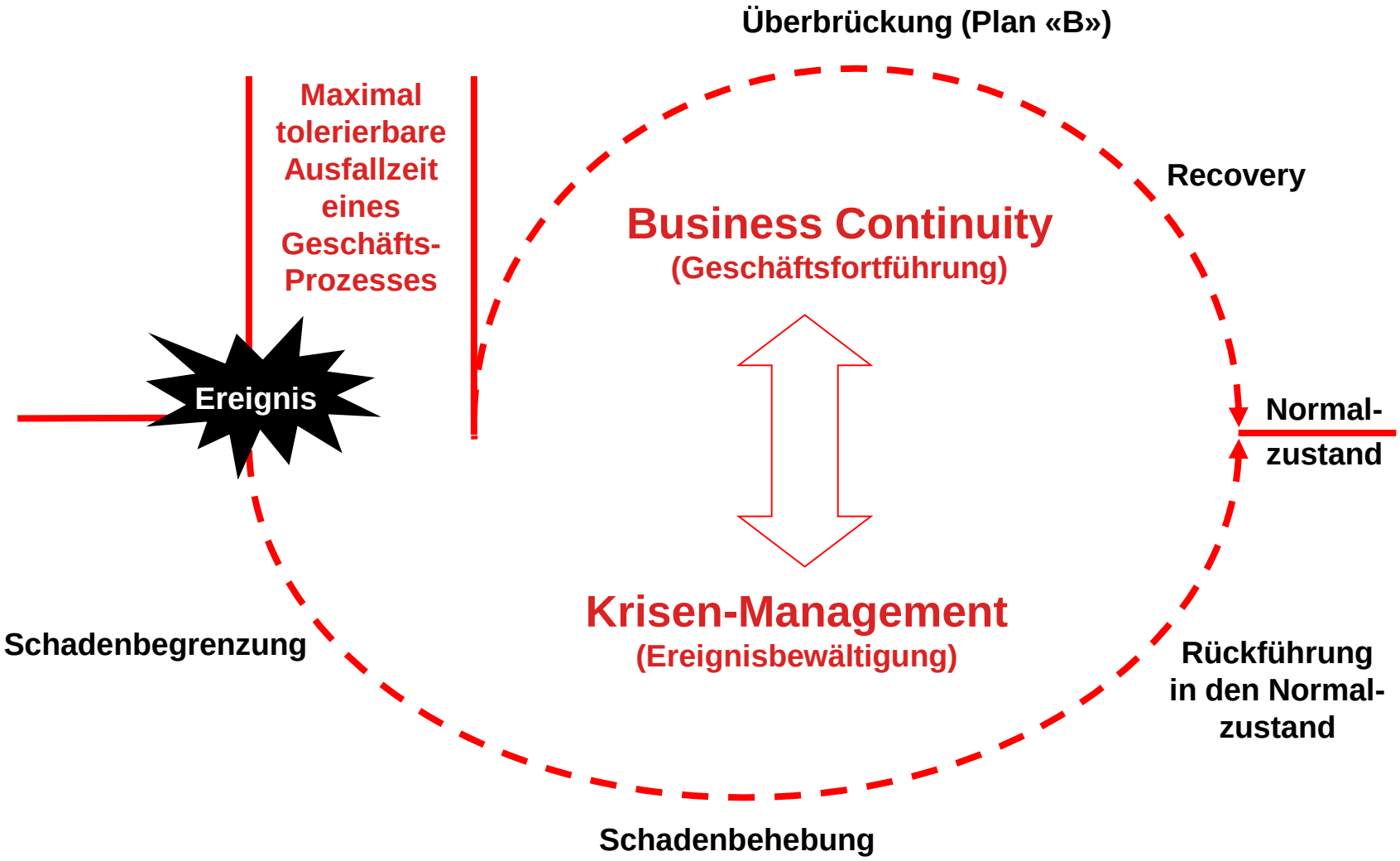
Risiko-Management und BCM



Business Continuity Management (BCM)

- Sicherung der Geschäftstätigkeit während und nach aussergewöhnlichen Umständen.
- Die Folgen schwerwiegender Beeinträchtigungen für das Unternehmen begrenzen (Geschäftsfort-führung).
- So rasch wie möglich den Normalzustand wieder herstellen (Ereignisbewältigung).

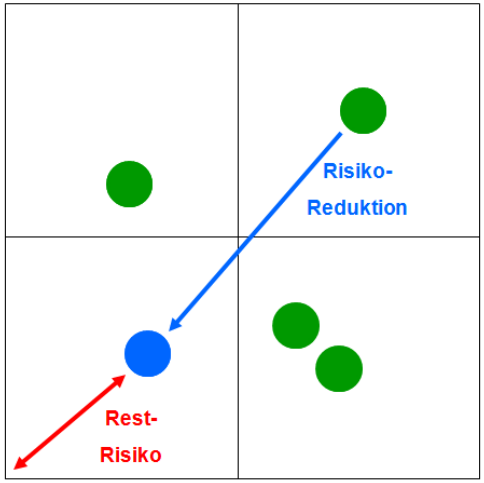
Die 2 Funktionen des BCMS



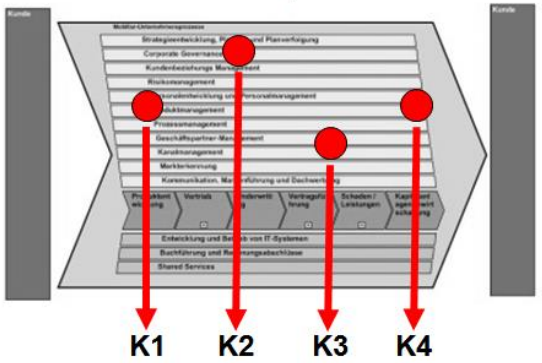
Schnittstellen

RM

Risikomatrix

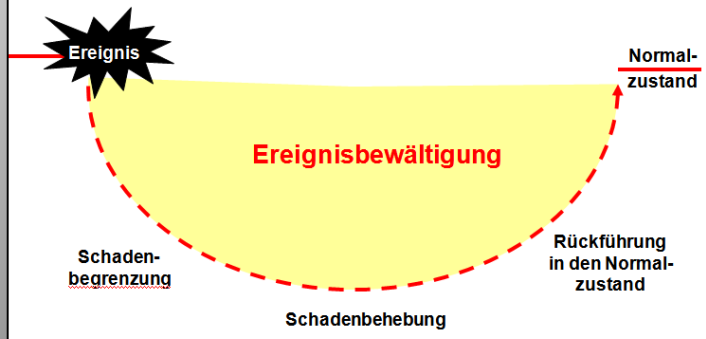


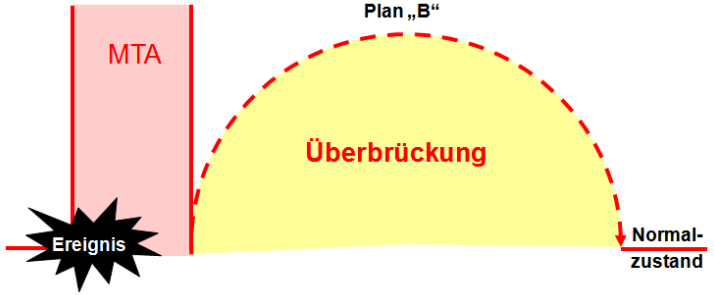
Geschäftsprozess



IKS

KM





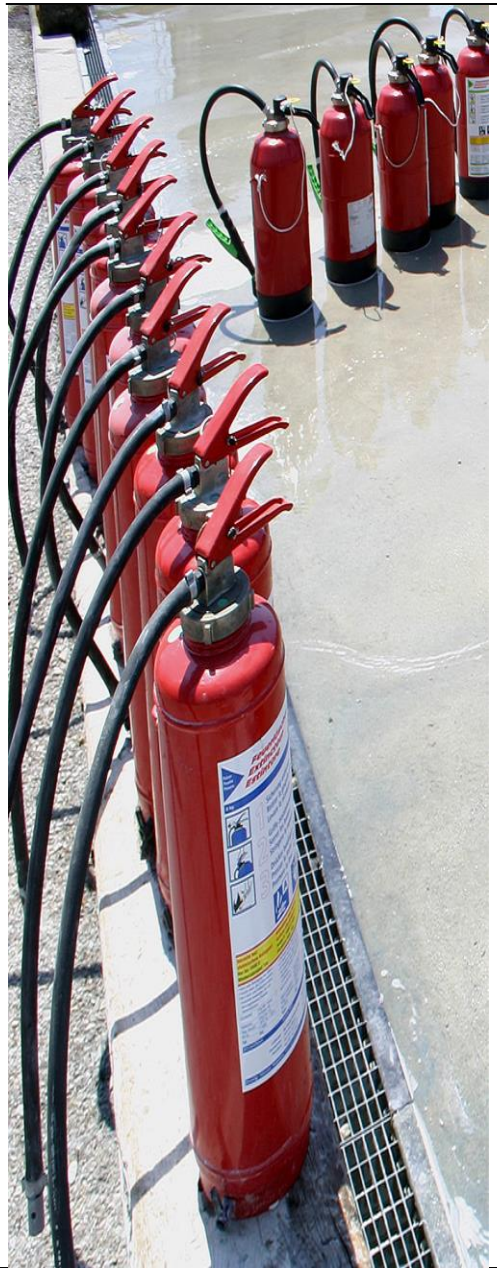
BC

Unterschiedliche Ziele von RM und BCM

- **Risiko-Management …**
- ermittelt mögliche Bedrohungen
- prüft und beurteilt Auswirkungen und Häufigkeit
- bewertet Tragbarkeit des Risikos
- **ist dafür verantwortlich, dass das Risiko möglichst klein ist (Häufigkeit und Ausmass)**

- **Business Continuity-Management …**
- bereitet sich auf das Rest-Risiko vor (Planung)
- evaluiert „Plan B“ (Continuity-Man.)
- bewältigt das eingetretene Ereignis (Krisen-Man.)
- **ist dafür verantwortlich, dass Ereignisse möglichst rasch und effizient behoben werden und die Geschäftsfortführung gesichert bleibt**

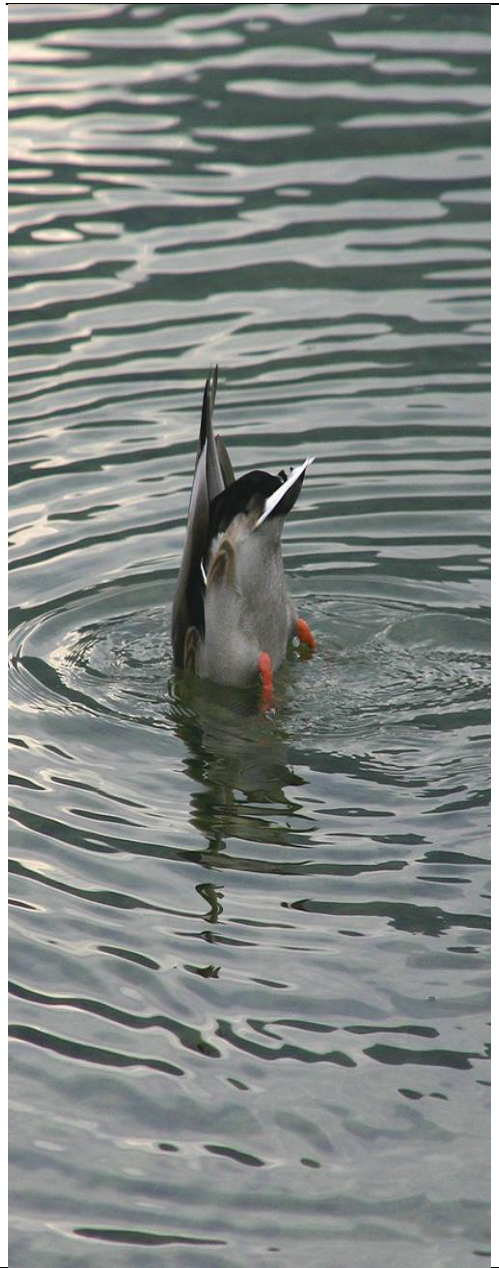
Unterschiede zwischen RM und BCM



Effiziente und effektive Bewältigung der Folgen eines Ereignisses stehen im Vordergrund, nicht Prävention oder die Verhinderung möglicher Risiken – wir gehen davon aus, jetzt ist es passiert!

Bewältigung
nicht Prävention

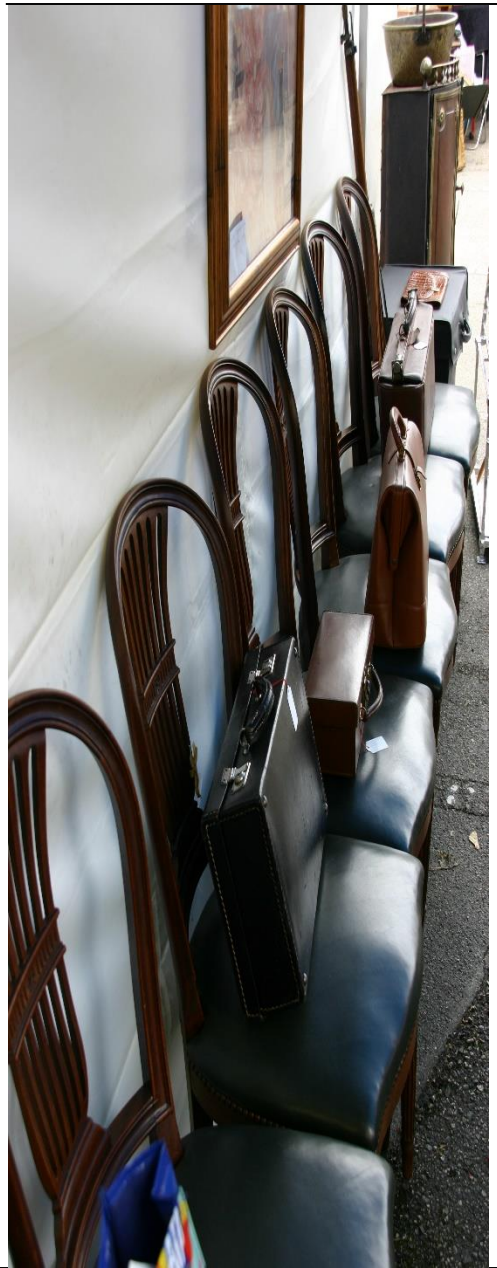
Unterschiede zwischen RM und BCM



Welches Ereignis warum eingetreten ist, interessiert im Moment nicht, sondern die Auswirkungen auf den Geschäftsbetrieb und die zeitkritischen Funktionen.

Auswirkungen
nicht Ursachen oder Risiken

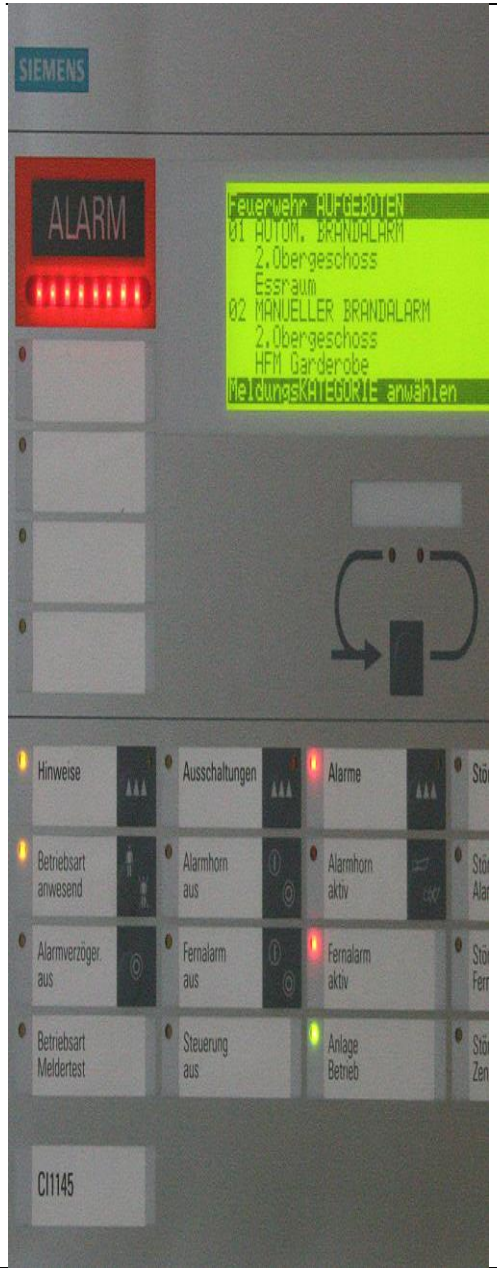
Unterschiede zwischen RM und BCM



Es gibt viele wichtige Geschäfts-prozesse, im Ereignisfall sind aber die zeitkritischen Funktionen prioritär – in der Regel sind dies die Geschäftsprozesse mit direktem Kundenkontakt.

Zeitkritisch
nicht (nur) wichtig

Unterschiede zwischen RM und BCM



Die Massnahmenplanung basiert auf den erforderlichen Ressourcen der zeitkritischen Funktionen (Facilities, Personal, Technik, Lieferanten), nicht auf Risiken oder Szenarien.

Ressourcen-Planung
nicht Szenarien-Planung

Risiko- und Business Continuity-Management

	Risiko-Management	Business Continuity Management
Zweck	**Schadensprävention**	**Schadensbewältigung**
Analysemethode	Risiko-Analyse	Impact-Analyse
Hauptparameter	**Wahrscheinlichkeit/Häufigkeit und finanzielle Auswirkungen**	**Alle Auswirkungen auf der Zeitachse**
Sichtweise	Mögliche Ereignisse, deren Ursachen und finanziellen Auswirkungen	Auswirkungen/Folgen auf die Geschäftsprozesse und deren Ressourcen
Ereignisarten	Alle Arten von Ereignissen mit finanziellen Auswirkungen	Auswirkungen, die erhebliche Betriebsstörungen verursachen
Ereignis-betrachtung	**Schadenausmass (normalerweise nur monetär)**	**Schadenentwicklung (auf der Zeitachse)**

Zusammenfassung

- RM und BCM sind komplementär, wir brauchen beides!
- Trotz bestem Risiko-Management bleibt immer ein Restrisiko, das für einen Betrieb nicht unerheblich sein kann.
- Die Bewältigung eines Ereignisses muss vorbereitet werden.
- Vorbereitet sein heisst
  - **Business Continuity** (Kontinuitätssicherung)
  - **Krisen-Management** (Ereignisbewältigung)
- Business Continuity Management heisst
  - Bewältigung, nicht Prävention
  - Auswirkungen, nicht Ursachen oder Risiken
  - Zeitkritisch, nicht (nur) wichtig
  - Ressourcen-, nicht Szenarien-Planung

Besten Dank

Albert Andrist

andrist beratungen

Arastrasse 16
3048 Worblaufen/Bern

079 330 28 01

albert.andrist@bluewin.ch

für Fragen klopfen Sie ruhig an !

© Albert Andrist

Quellenhinweise

- **ISO 22301**
  Societal security – Business continuity management systems – Requirements and Guidance

- Grafiken: © A. Andrist / Protekta Risiko-Beratungs-AG, Bern
- Bilder: © A. Andrist, Worblaufen