GESELLSCHAFT FÜR INFORMATIK E.V.
Zukunft gestalten.

BCM im Überblick

GI FG SECMGT
Frankfurt 26.06.2009

Bernd Ewert

consequa GmbH

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

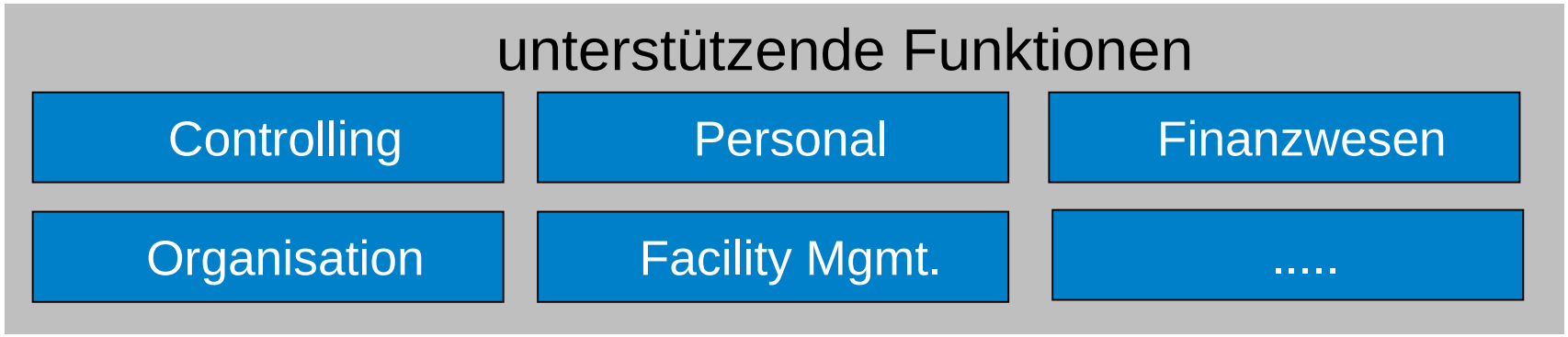
Agenda

- Wer oder was ist Business Continuity?
- Gesetze und Vorschriften für BCM
- Normen und Standards für BCM
- BCM als Querschnittsprozess

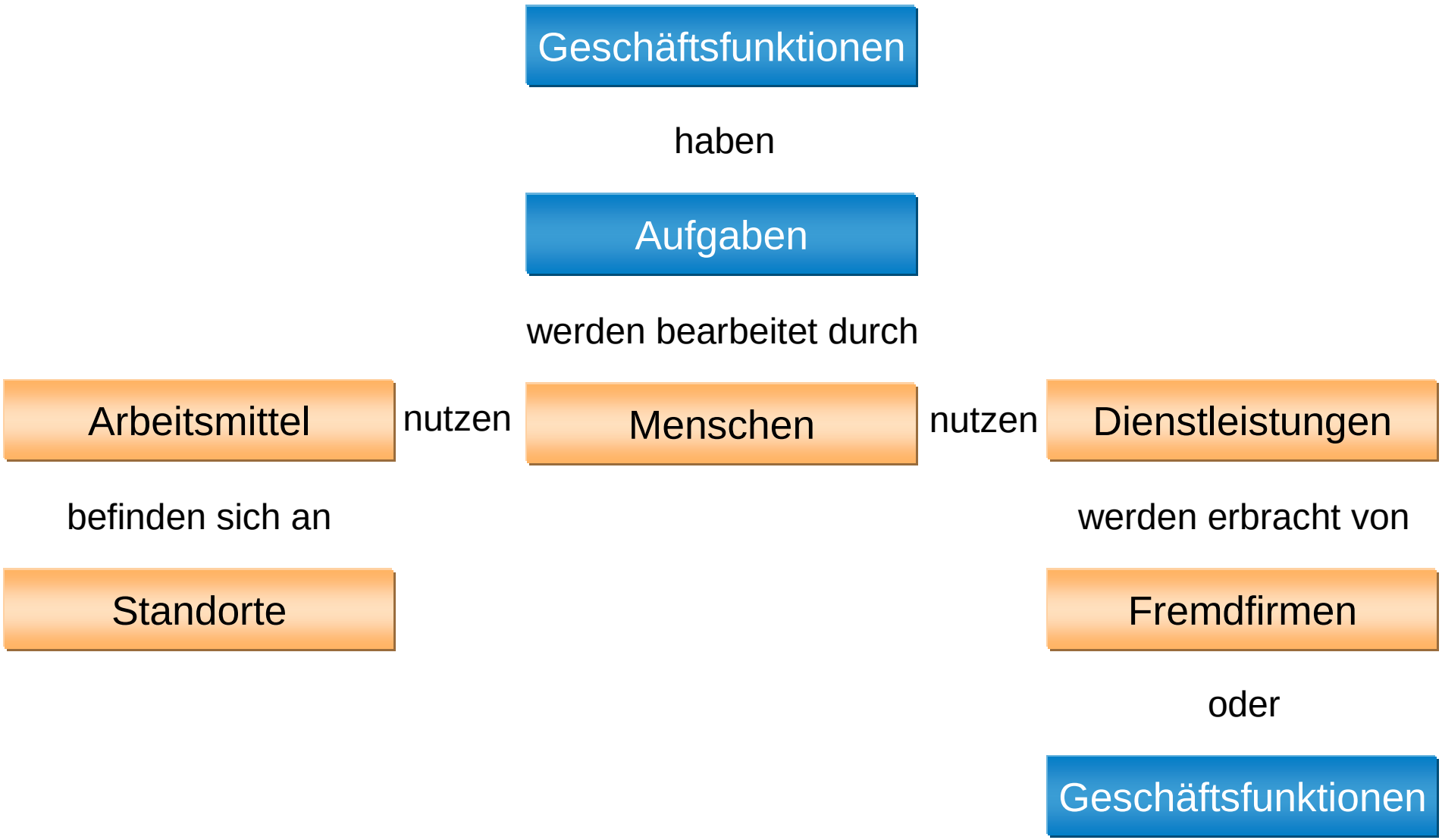
Agenda

- Wer oder was ist Business Continuity?
- Gesetze und Vorschriften für BCM
- Normen und Standards für BCM
- BCM als Querschnittsprozess

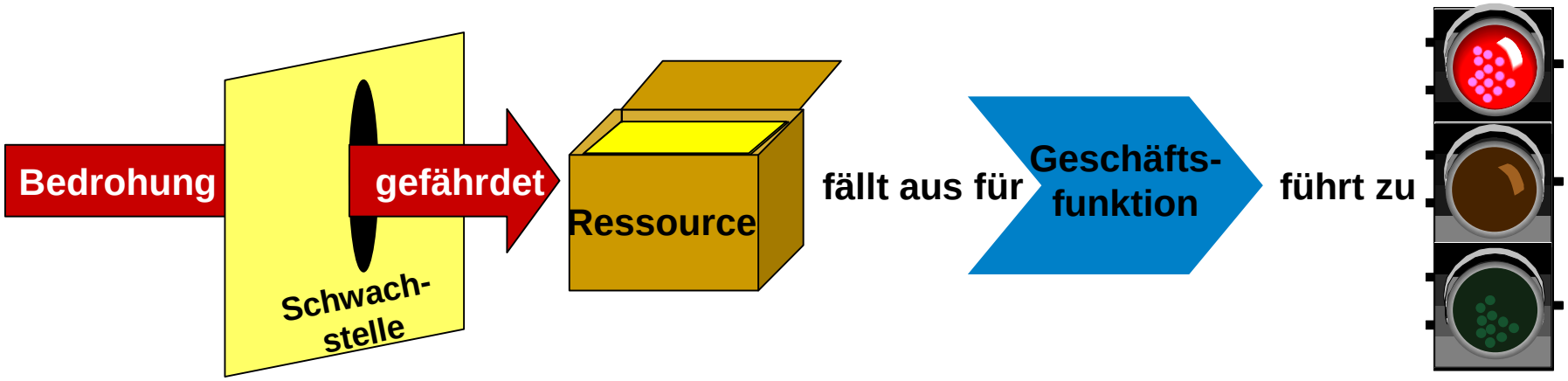
Was ist Business?



Was wird für Kontinuität benötigt?



Gefahren und Schutz für Kontinuität



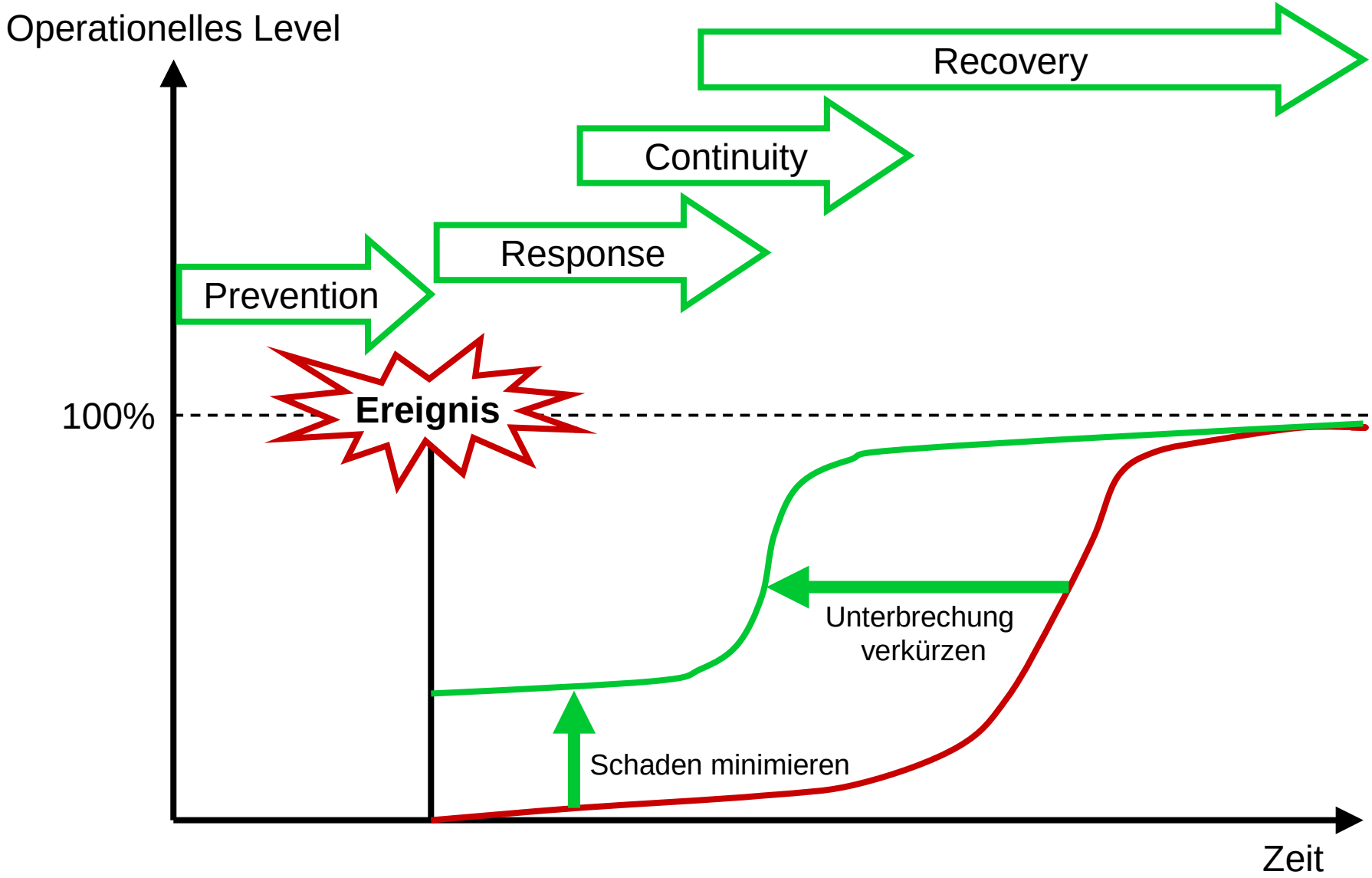
Bedrohungs-wahrscheinlichkeit senken — präventiv

Schwachstelle beseitigen — präventiv

Schaden begrenzen — reaktiv

Schaden begrenzen — reaktiv

Ziele für Business Continuity (ISO/PAS 22399)



Warum Business Continuity Management?

To be or not to be (anymore),
that is the (BCM) question ...

Quinet Gregory frei nach Shakespeare

Agenda

- Wer oder was ist Business Continuity?
- Gesetze und Vorschriften für BCM
- Normen und Standards für BCM
- BCM als Querschnittsprozess

Vorschriften für Unternehmen allgemein

+

Gesetz / Dokument	Paragraphen / Abschnitte	Inhalt
BGB	276, 278, 823, 831	Verantwortlichkeit, Schadensersatzpflicht
AktG	91, 93, 116	Risikoüberwachung, Sorgfaltspflicht
GmbHG	43	Sorgfaltspflicht
HGB	317, 321	Prüfung der Risikoüberwachung
RS FAIT 1	3.1, 4.2	Ordnungsmäßige elektronische Buchführung
RS FAIT 2	2.2	Ordnungsmäßiger Electronic Commerce
RS FAIT 3	7.2	Ordnungsmäßige elektronische Archivierung

- Sarbanes-Oxley-Act

Vorschriften für Finanz-Infrastrukturen

+ BaFin

Gesetz / Vorschrift	Paragraphen / Abschnitte	Inhalt
KWG	25a, 29	Ordnungsgemäße Geschäftsorganisation
MaRisk	AT 2.2, AT 7.1, AT 7.2, AT 7.3	Operationelle Risiken, Personal, technisch-organisatorische Ausstattung, Notfallkonzept
VAG	64a, 104s	Ordnungsgemäße Geschäftsorganisation
MaRisk VA	5, 7.2.2, 9	Operationelles Risiko, Ablauforganisation, Notfallplanung

- internationale Vereinbarung Basel II
- EU-Richtlinie Solvency II

Vorschriften für Versorgungs-Infrastrukturen

+ Bundesnetzagentur

Gesetz / Vorschrift	Paragraphen / Abschnitte	Inhalt
TKG	109	Technische Schutzmaßnahmen für Telekommunikation
PTSG	3, 5	Vorsorgeplanungen für Post und Telekommunikation
EnWG	49, 50, 53a	Energieanlagen, Versorgungssicherheit

- Richtlinie zu Kritischen Infrastrukturen (EPCIP/EPSKI)

Die Bundesregierung

- Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI)
- Nationale Strategie zum Schutz Kritischer Infrastrukturen

Agenda

- Wer oder was ist Business Continuity?
- Gesetze und Vorschriften für BCM
- Normen und Standards für BCM
- BCM als Querschnittsprozess

Standards für IT-Management und Inf.-Sicherheit

IT Governance Institute® + OGC + ISO + Bundesamt für Sicherheit in der Informationstechnik

Norm / Standard	Abschnitte	Inhalt
CobiT 4.1 (2007)	PO7, DS4	Manage IT Human Ressources, Ensure Continuous Service
ITIL V3 Service Design (2007)	4.5	IT Service Continuity Management
ISO/IEC 20000 (-1 und -2) (2005)	6.3	Service Continuity Management
ISO/IEC 27002 (2005)	14	Business Continuity Management
IT-Grundschutz-Kataloge	B 1.3, M 6	Notfallvorsorge-Konzept, Maßnahmenkatalog Notfallvorsorge

Standards für IT Continuity Management

+ nationale Normungsorganisationen

Norm / Standard	Herkunft	Inhalt
ISO/IEC 24762	International (ISO 2008)	Information and Communication Technology Disaster Recovery Services (für DR-Service-Provider)
BS 25777	Großbritannien (BSI 2008)	Information and Communications Technology Continuity Management
SP 800-34	USA (NIST 2002)	Contingency Planning for Information Technology Systems
SS 507	Singapur (SPRING 2008)	Information and Communications Technology Disaster Recovery Services

Standards für Business Continuity Management

Angloamerikanische Organisationen

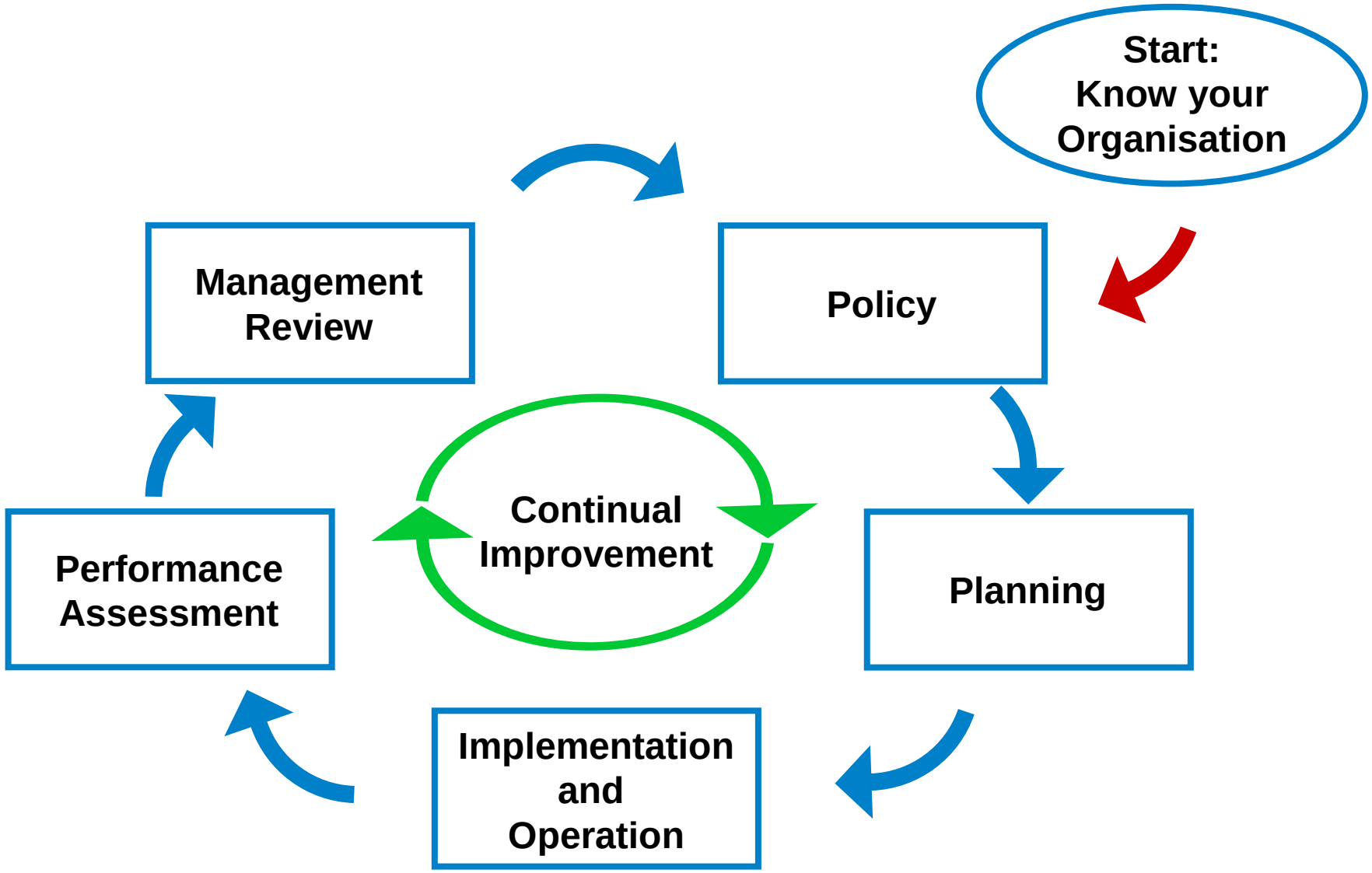
Norm / Standard	Herkunft	Inhalt
BS 25999 (-1 und -2)	Großbritannien (BSI 2006/07)	Business Continuity Management
BCI GPG	Großbritannien (BCI 2008)	Business Continuity Management
NFPA 1600	USA (NFPA 2004)	Disaster / Emergency Management and Business Continuity Programs
ASIS GDL BC	USA (ASIS 2005)	Business Continuity: Emergency Preparedness, Crisis Management, and Disaster Recovery
ASIS SPC.1	USA (ANSI 2009)	Organizational Resilience: Security, Preparedness, and Continuity Management Systems
HB 292	Australien (SA 2006)	Business Continuity Management

Standards für Business Continuity Management

+ nicht-angloamerikanische Organisationen

Norm / Standard	Herkunft	Inhalt
ISO/PAS 22399	International (ISO 2007)	Incident Preparedness and Operational Continuity Management
SS 540	Singapur (SPRING 2008)	Business Continuity Management
INS 24001	Israel (INS 2007)	Security and Continuity Management Systems
BCPDG / BCG	Japan (Gov. 2005)	Business Continuity
BSI 100-4	Deutschland (BSI 2008)	Notfallmanagement

Management-Zyklus nach ISO/PAS 22399



Agenda

- Wer oder was ist Business Continuity?
- Gesetze und Vorschriften für BCM
- Normen und Standards für BCM
- BCM als Querschnittsprozess

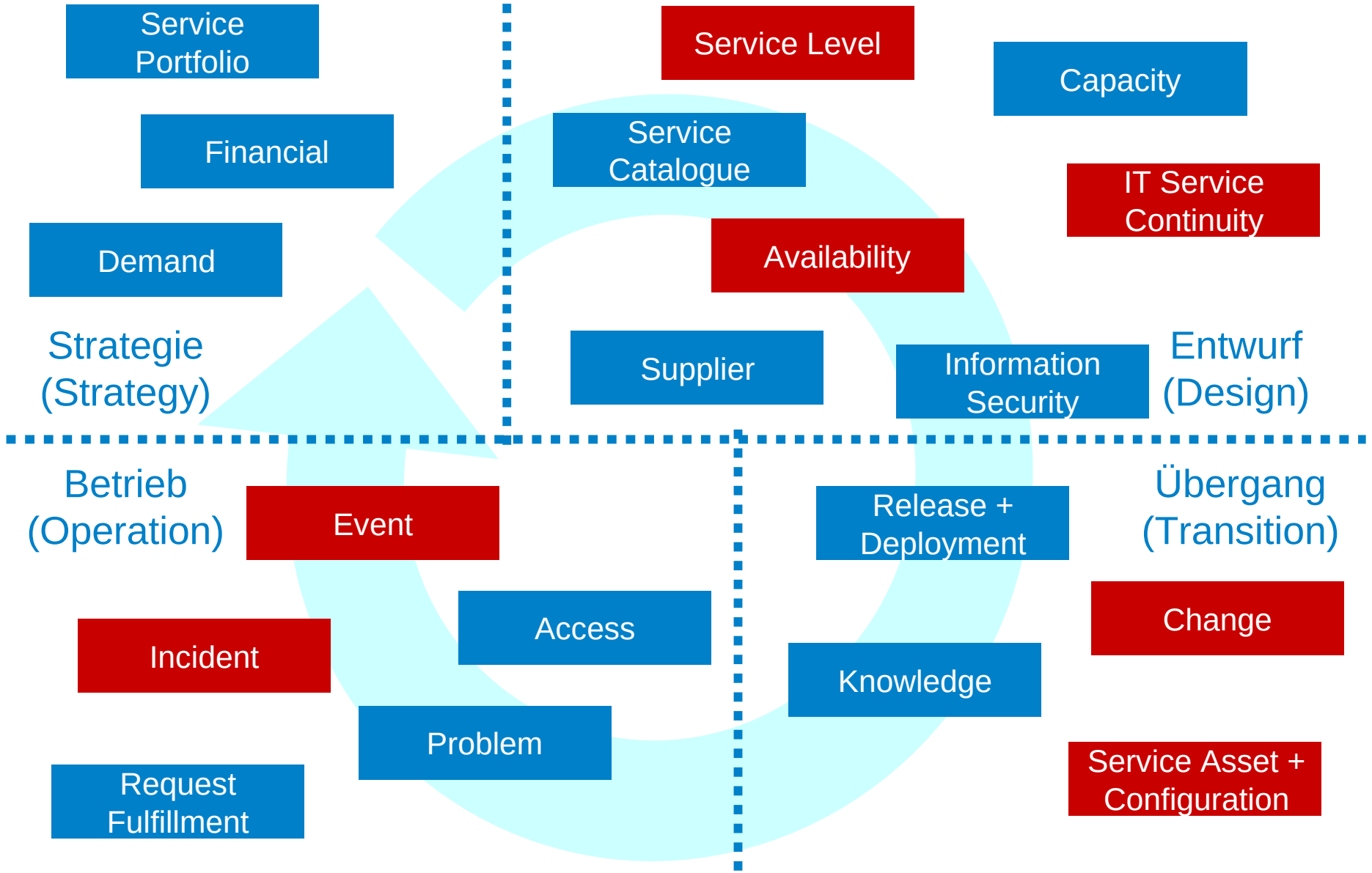
Einbettung des BC in das Unternehmen

- Compliance-Management
  - Beachtung rechtlicher Anforderungen
- Risiko-Management
  - Justierung an eigenen Anforderungen
- Krisen-Management
  - Führungsstruktur in Situationen mit Gefährdung der BC
- Qualitäts-Management
  - Kontinuität als Bestandteil der Verlässlichkeit
- Sourcing-Management
  - BC-Dienstleister als wesentlicher Geschäftspartner

BC und andere Sicherheitsdisziplinen

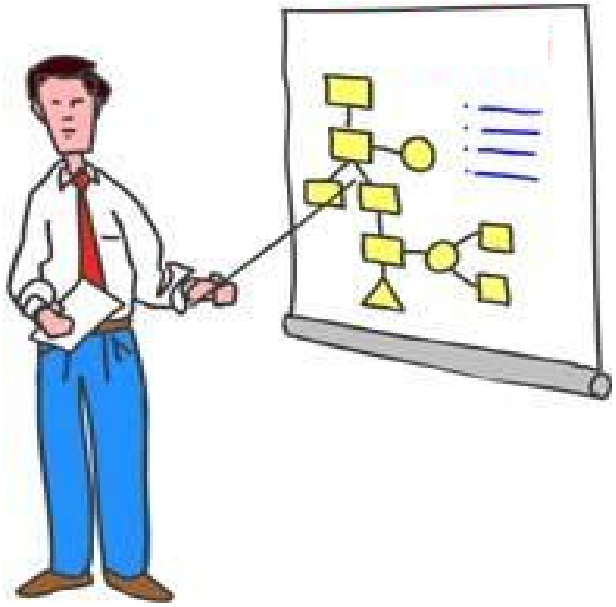
- Business Continuity
  - sichert die angemessene Verfügbarkeit und Wiederherstellung **kritischer Ressourcen**, die zur Ausübung kritischer Geschäftsfunktionen benötigt werden
- Information Security
  - sichert angemessene Verfügbarkeit, Vertraulichkeit, Integrität, Verbindlichkeit der genutzten **Informationen**
- 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

IT Service Continuity und Nachbarprozesse



(nach ITIL V3)

Vielen Dank
für Ihre Aufmerksamkeit!



consequa

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