

Notfallmanagementforum 2008

ISO/PAS 22399:2007

Lothar Goecke





- 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.





Unternehmensziele - Leistungen der consequence

Compliance

Risiko-
beherrschung

Ordnungs-
mäßigkeit

Wirtschaft-
lichkeit

Qualität

Business Continuity

BC-Leitfaden

Business Impact Analyse

BC-Konzept

BC-Pläne

BC-Test

BC-Review

Information Security

IS-Leitlinie

IS-Richtlinien

IS-Risikoanalyse

IT-Infrastruktur

IS-Audit

Service Quality

IT-Strategie

SLAs

IT-Prozesse

Krisenmanagement

KM-Leitfaden

KM-Übung

Datenschutz

DS-Organisation

DS-Audit



Agenda

- Inhalt der ISO/PAS 22399
- ISOPAS 22399 IPOCM-Framework
vs. BS25999 PDCA-Lifecycle
- Relevanz des ISO-Standards in Deutschland
neben BSI 100-4 und BS 25999
- Zusammenfassung



Public Available Specification - Standard

- Technical committees bereiten Standards vor. Vorschläge müssen mit 75% Stimmanteilen angenommen werden.
- Bei dringenden Marktbedürfnissen können diese Gremien auch ISO Public Available Specifications (ISO/PAS) 50%ger Mehrheit verabschiedet werden.
- Bei 2/3 Mehrheit entsteht ein ISO Technical Specification (ISO/TS)
- TS und PAS werden nach 3 Jahren reviewed und
 - beibehalten
 - zum Standard erhoben oder
 - gelöscht



ISO TC 223 – weitere Themen

- Essential information and data requirements for command and control
- Inter/intra organizational warning procedures
- Principles for command, control, coordination and cooperation in resolving incidents
- Framework for standards
- Vocabulary
- Systems requirements for interoperability.



Einbezogene internationale Standards

- Die ISO/PAS 22399 basiert auf Best Practices aus fünf Nationen. Es sind Teile enthalten von
- NFPA 1600:2400, amerikanischer Standard,
- BS 25999-1:2006, des britischer Standard,
- HB 221:2004, australischer Standard,
- INS 24001:2007, sraelischer Standard,
- Business Continuity Plan Drafting Guideline, Ministry of Economy, Trade and Industry of Japan 2005 und
- Business Continuity Guideline, Central Disaster Management Council, Cabinet Office, Government of Japan, 2005.
- Normativer Verweis auf: ISO/IEC Guide 73:2002 Risk management – Vocabulary – Guidelines for use in standards

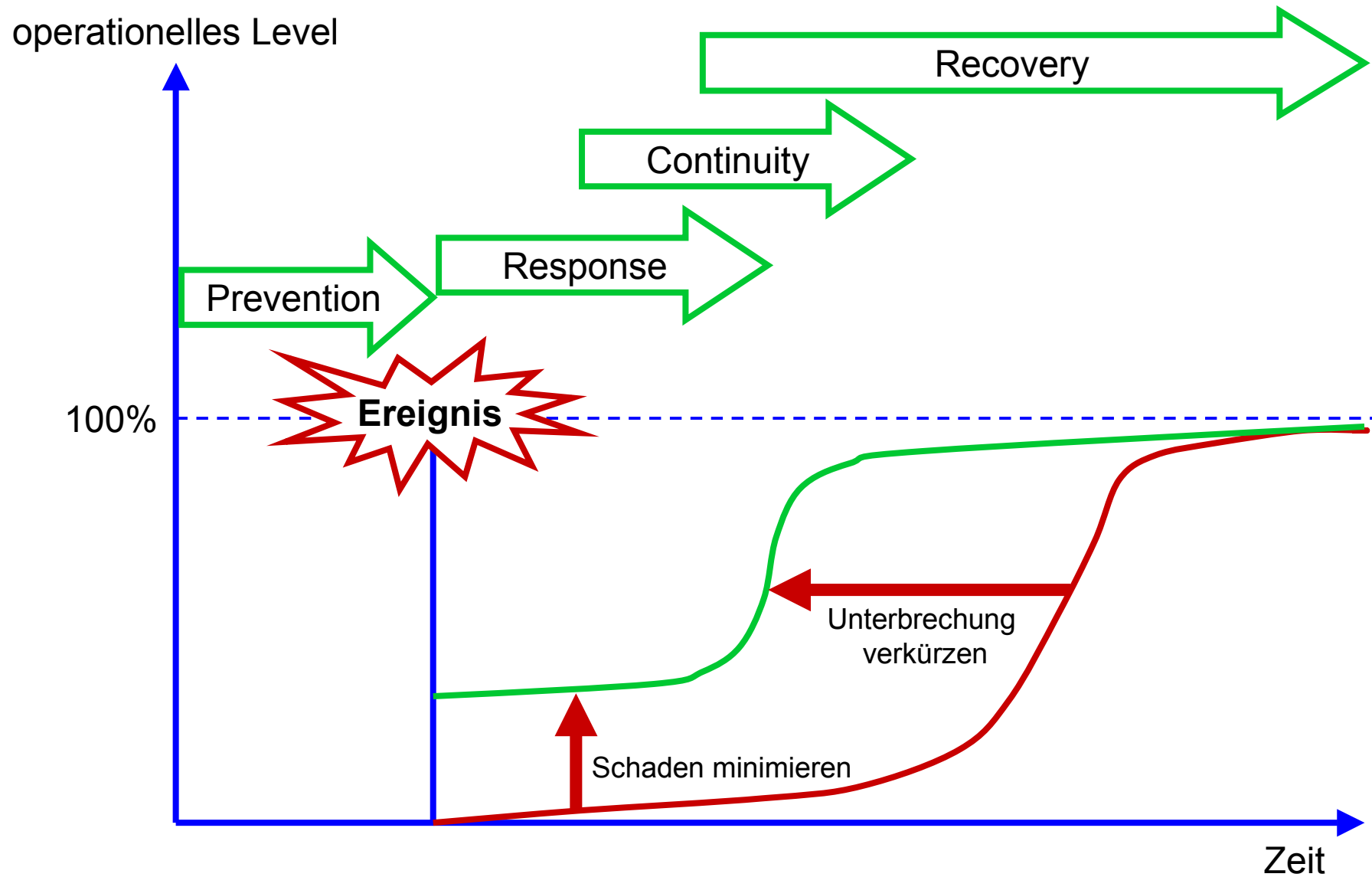


Methode

- Statt PDCA lifecycle IPOCM framework:
 - **I**ncident
 - **P**reparedness and
 - **O**perational (business)
 - **C**ontinuity
 - **M**anagement.
- operational continuity geeignet für
 - öffentlich, privat und non-profit
 - B2B und B2C
 - alle Firmengrößen
- Definition:
Ganzheitlicher Managementprozess, der Bedrohungen und Schäden einer Organisation identifiziert und ein Rahmenwerk zur Minimierung der Auswirkungen bietet.



Konzept



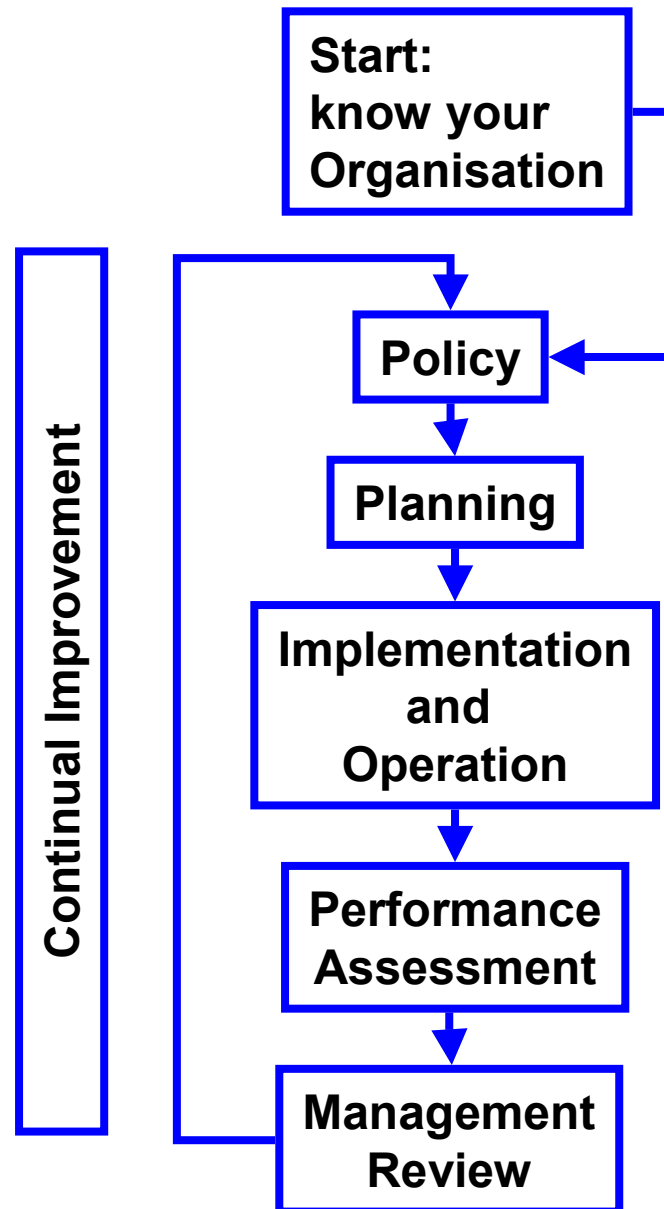


Begriffe und Definitionen

- **critical activity**
- **consequence**
- **crisis**
- **disaster**
- **disruption**
- **emergency**
- **exercising**
- **event**
- **hazard**
- **impact**
- **impact analysis**
- **incident**
- **incident management plan**
- **incident preparedness**
- **IPOCM**
- **IPOCM policy**
- **mitigation**
- **mutual aid agreement**
- **operational continuity (OC)**
- **operational continuity management (OCM)**
- **operational continuity management program**
- **operational continuity management team**
- **operational continuity plan (OCP)**
- **operational continuity strategy**
- **operational continuity team**
- **organization**
- **prevention**
- **probability**
- **recovery time objective (RTO)**
- **residual risk**
- **resilience**
- **response program**
- **risk**
- **risk acceptance**
- **risk assessment**
- **risk communication**
- **risk criteria**
- **risk management**
- **risk reduction**
- **risk transfer**
- **risk tolerance**
- **risk treatment**
- **simulation exercise**
- **stakeholder (interested party)**
- **tabletop exercise**
- **testing**
- **threat**
- **top management**



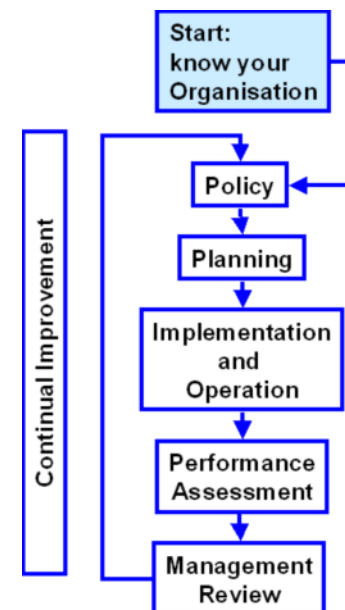
Methode





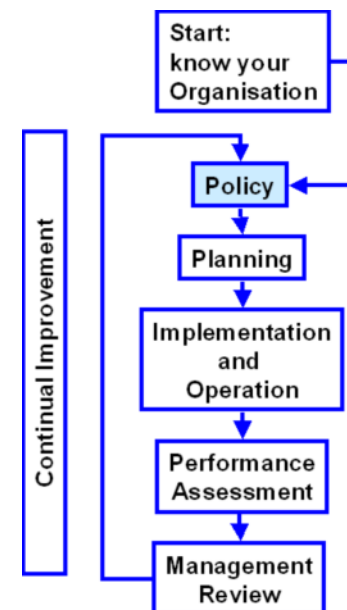
Start

- Geltungsbereich festlegen
 - Basis ist
 - Risikomanagement
 - Unternehmens-Strategien
 - Business-Pläne
 - Balanced Scorecards
 - SWOT-Analysen
 - kritische operationelle Ziele identifizieren
 - „grobe Richtung“ vorgeben
- IPOCM Programm begründen durch z.B.
 - Ereignisse, Risiken, Trends, Haftung, Verantwortung Schadensabwendung



Policy

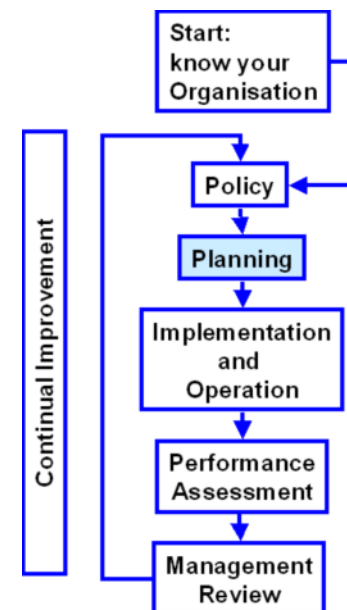
- Policy entwickeln
 - vom Management getrieben
 - Management kommuniziert ins Unternehmen
 - Management ist aktiv beteiligt
- Policy review
 - lessons learned
 - Veränderungen einbeziehen
 - Risikoprofil berücksichtigen
 - Personalveränderungen berücksichtigen
 - compliance aktualisieren
- IPOCM Organisation etablieren
 - Koordinator einsetzen (initial: Projektleiter)





Planning

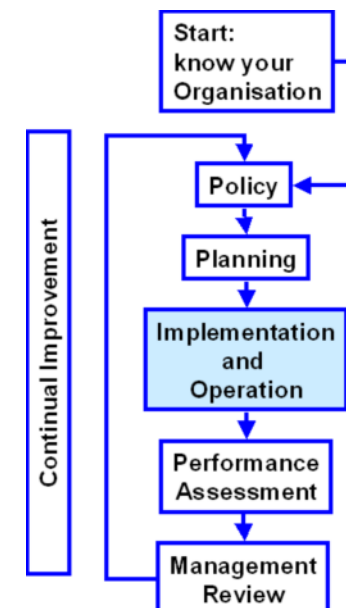
- Gesetze und Richtlinien
- Risikoanalyse
- Business Impact Analyse (RTO)
- IPOCM Methode
 - Prävention und Vermeidung
 - Reaktion
 - Sofortmaßnahmen (emergency response)
 - Kontinuität (continuity response)
 - Wiederherstellung (recovery response)





Implementation and Operation

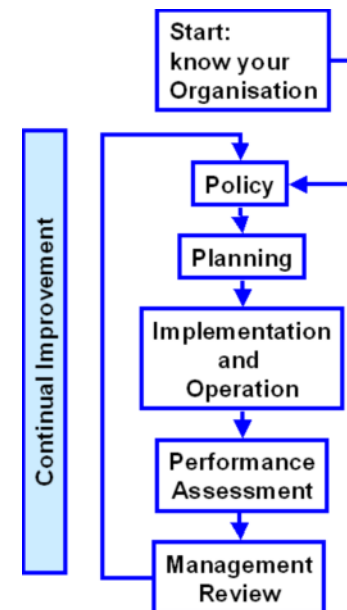
- Kapazitäten
- Rollen
- Verantwortlichkeiten
- Kompetenzen
- Sensibilisierung
- Training
- Kommunikation (extern und intern)
- Controlling (operationell und finanziell)





Continual Improvement

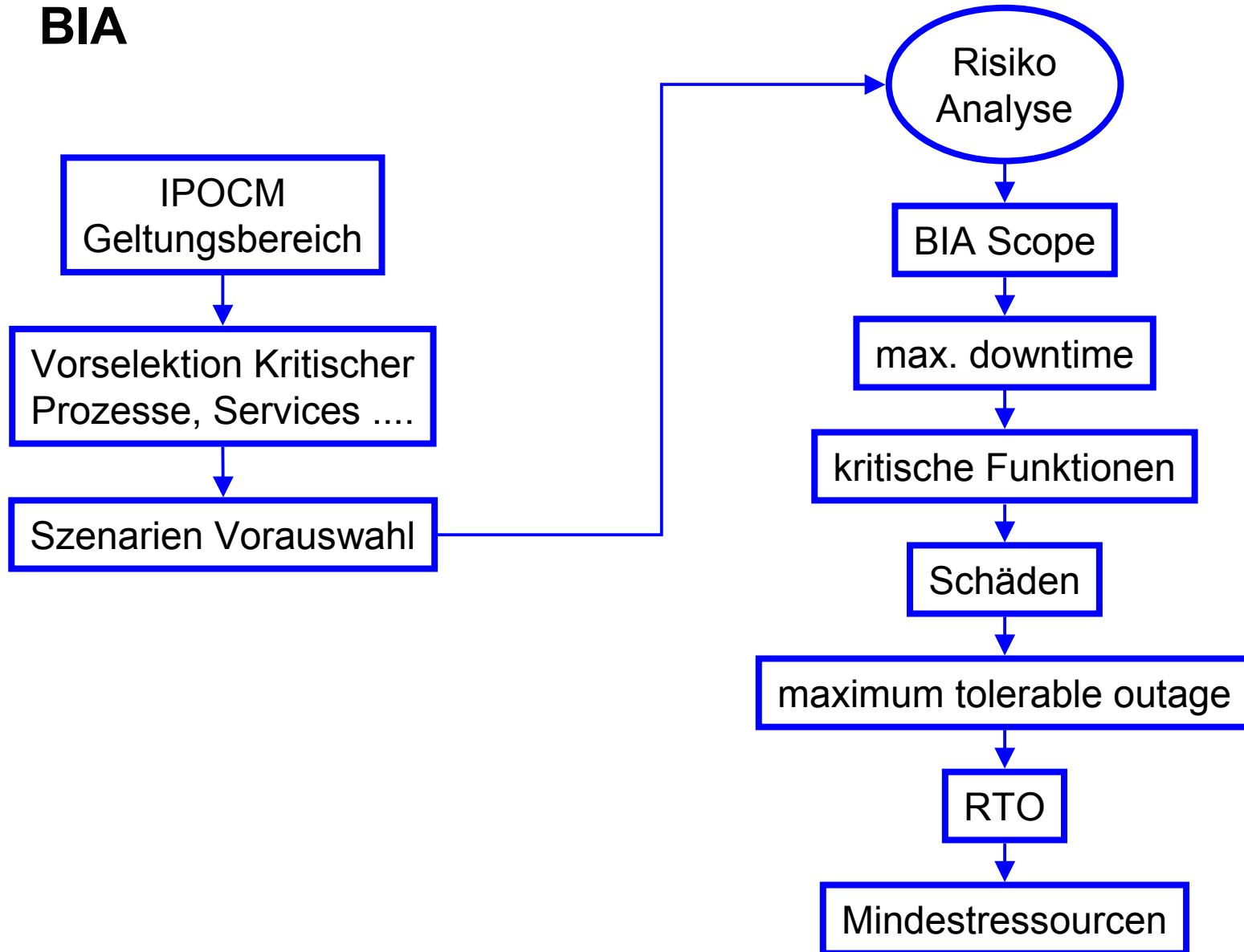
- IPOCM
- Prozess statt Projekt
- Einbettung in alle notwendigen Unternehmensabläufe





Anhang A (informell)

BIA





Anhang B (informell)

Emergency response management program

- Rollen und Verantwortung
- Ressourcen Anforderungen
- Zusätzliche Informationen



Anhang C (informell)

Continuity management program

- Konsolidierung und Dokumentation der operational continuity management (OCM) Pläne
- Ausstattung, Versorgung und Versorgungsketten
- OCM plan strategy options



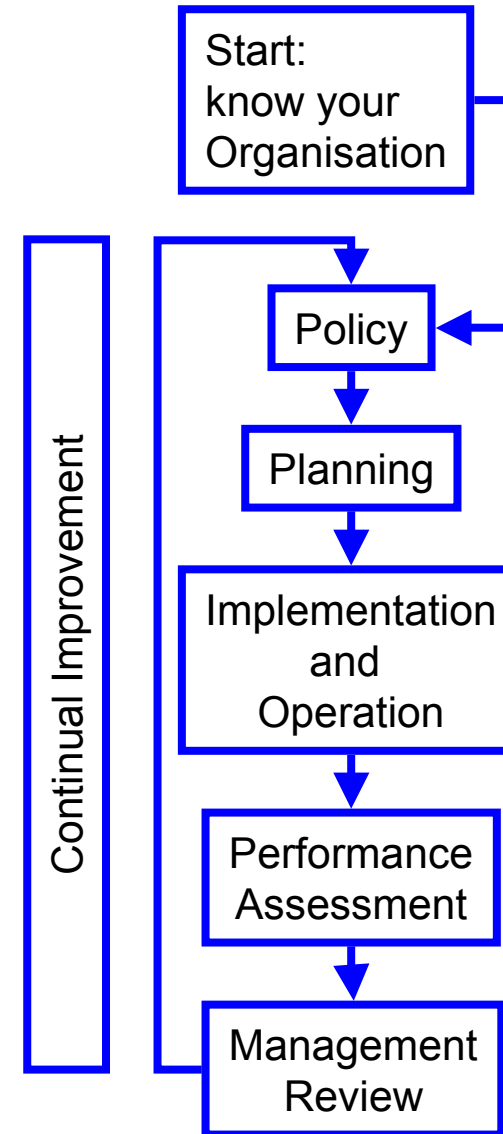
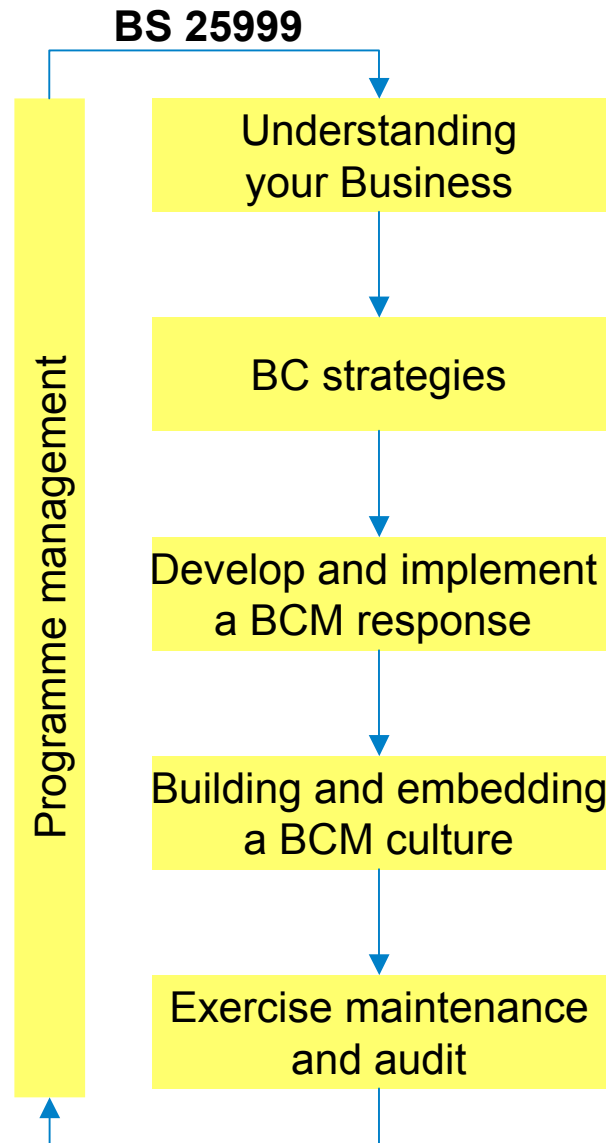
Anhang D (informell)

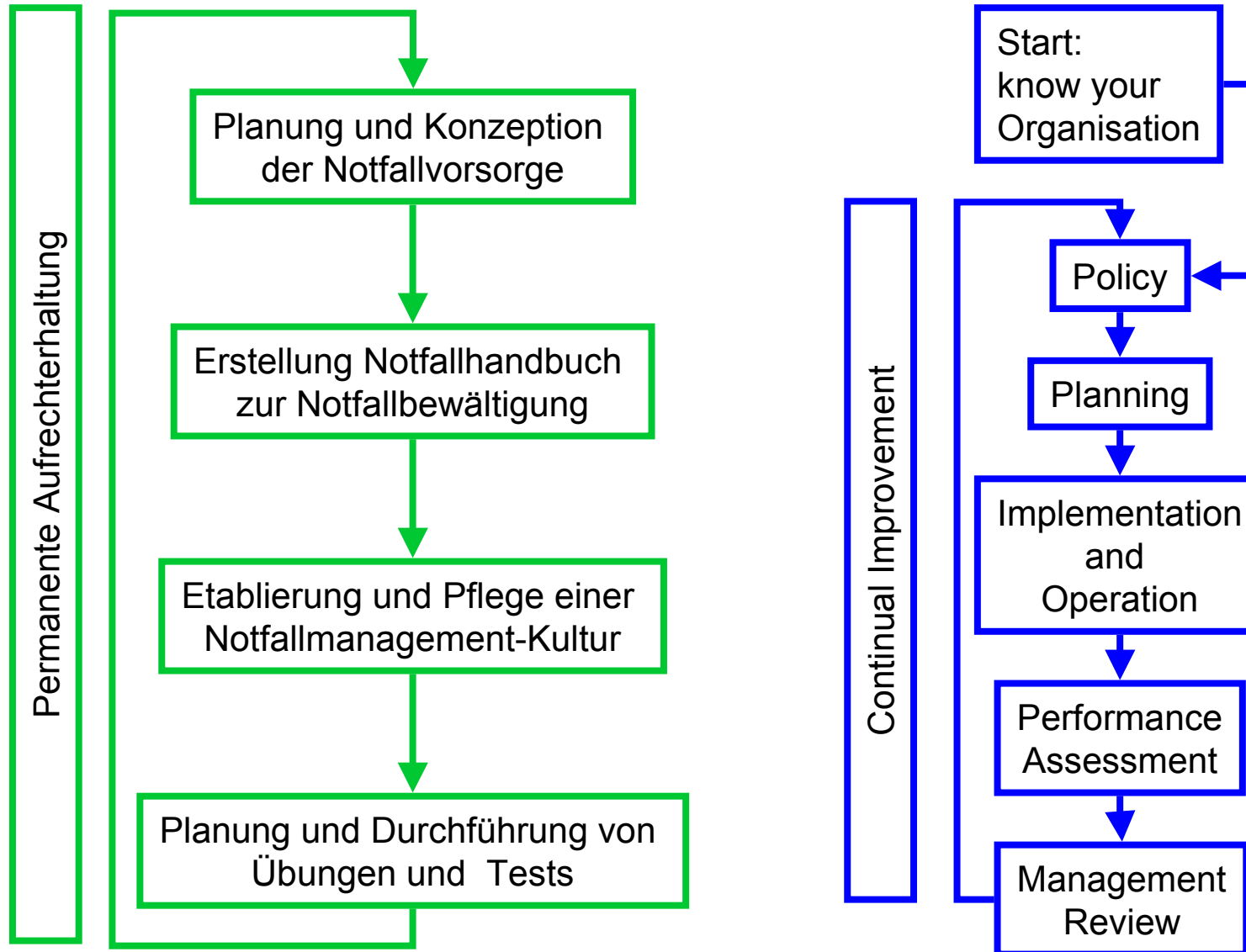
Building an incident preparedness and operational continuity culture

- Elements
 - Management Unterstützung
 - Veröffentlichung der IPOCM Policy
 - gemeinsames Verständnis aller Beteiligten
 - Übernahme der Verantwortung durch die Unternehmensleitung
 - Einbeziehen der mittleren Führungsebene
 - Schulung, Sensibilisierung und Übungen



25999 - 22399





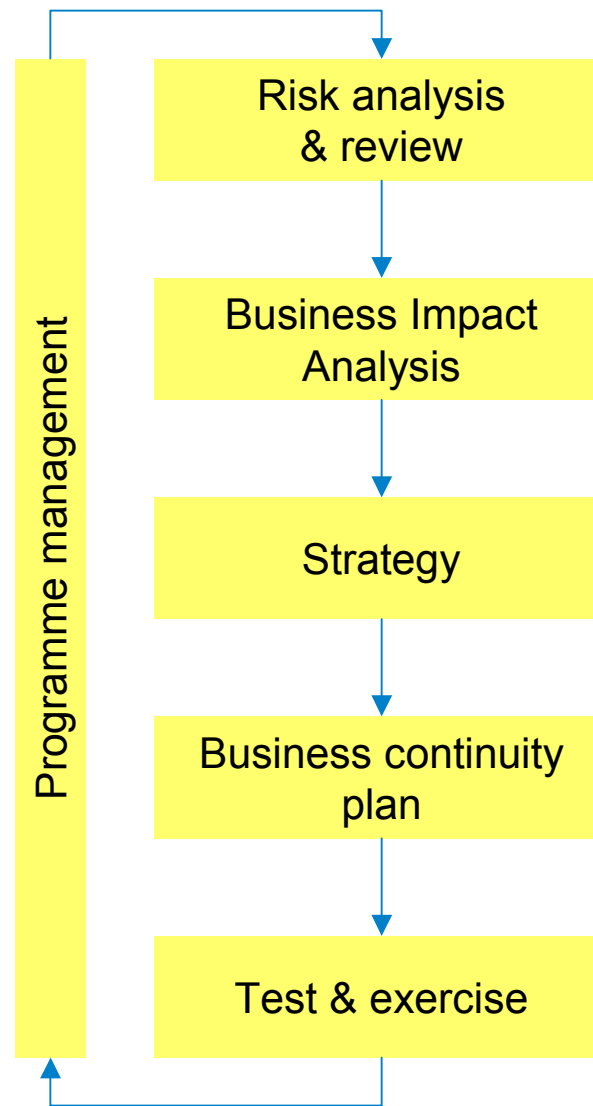


HB292 - Australien





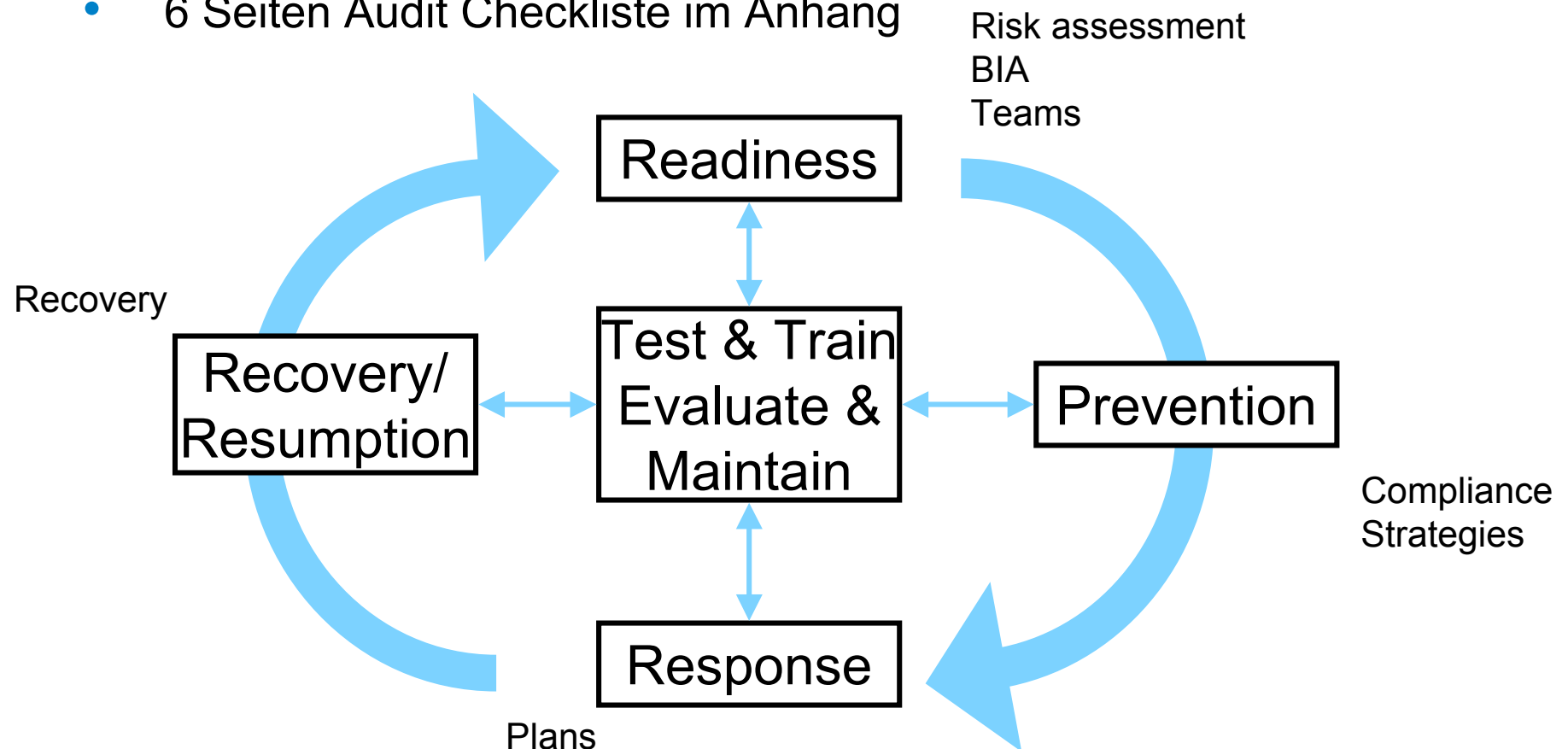
TR 19 - Singapur





ASIS GDL BC 01 2005 (USA, z.Z. in Überarbeitung)

- **Business Continuity Guideline**
A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery
- Die ASIS formuliert die Standards für die ANSI
- 6 Seiten Audit Checkliste im Anhang



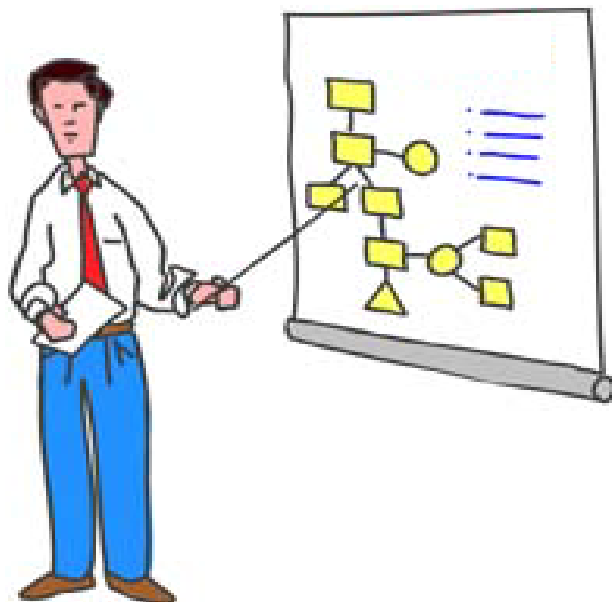


22399 - Lob und Tadel

- nicht zur Zertifizierung vorgesehen
- Beispiel für Risikoanalyse und BIA
- Schaden im Zeitverlauf (<-> RIA)
- Anforderungen ohne RPO
- Abgrenzung / Schnittstelle zum Krisenmanagement
- Dokumentationsstruktur
- Einbettung in das Risikomanagement
- Begriffsdefinitionen
- Wiederherstellungsplan
- TR19 Technical Reference for BCM (Singapore)
- HB 221:2004 wurde HB 292:2006



Vielen Dank für Ihre Aufmerksamkeit!



Dipl.-Math.

Lothar Goecke

Geschäftsführer

consequa GmbH
Süderstraße 73
20097 Hamburg
www.consequa.de

Tel.: 040 / 78 89 70 62
Fax: 040 / 78 89 70 66
Mob: 0171 / 863 50 17
lothar.goecke@consequa.de