Notfallmanagement Forum 2011

Nürnberg, 12.10.2011

Der ISO Standard 27031
und
Kennzahlen im BCM

Lothar Goecke

consequa
continuity · security · quality

Agenda

- ISO 27031 – Guidelines for information technology readiness for business continuity
- Kennzahlen für das BCM im ISO 27031
- Verwendung(smöglichkeit) des CERT® Resilience Management Models des Software Engineering Institute der Carnegie Mellon University für BCM Kennzahlen
- BCM Kennzahlen nach ISO 27004
- Zusammenfassung

BS ISO/IEC 27031:2011

Information technology

- Security techniques -

Guidelines for information and communication technology readiness for business continuity

Vorläufer ist:

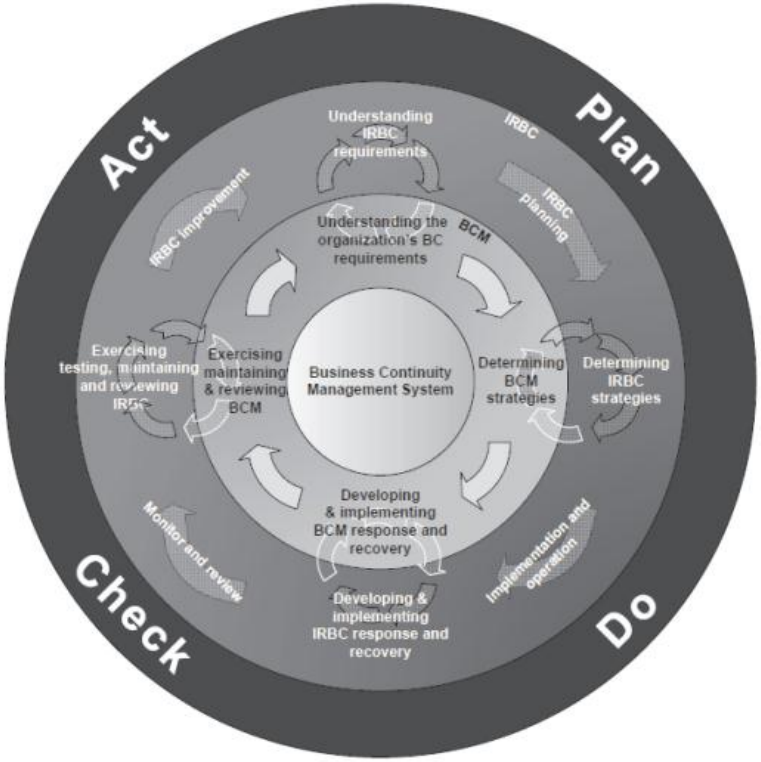
BS 25777:2008

Information and communications technology

continuity management – code of practice

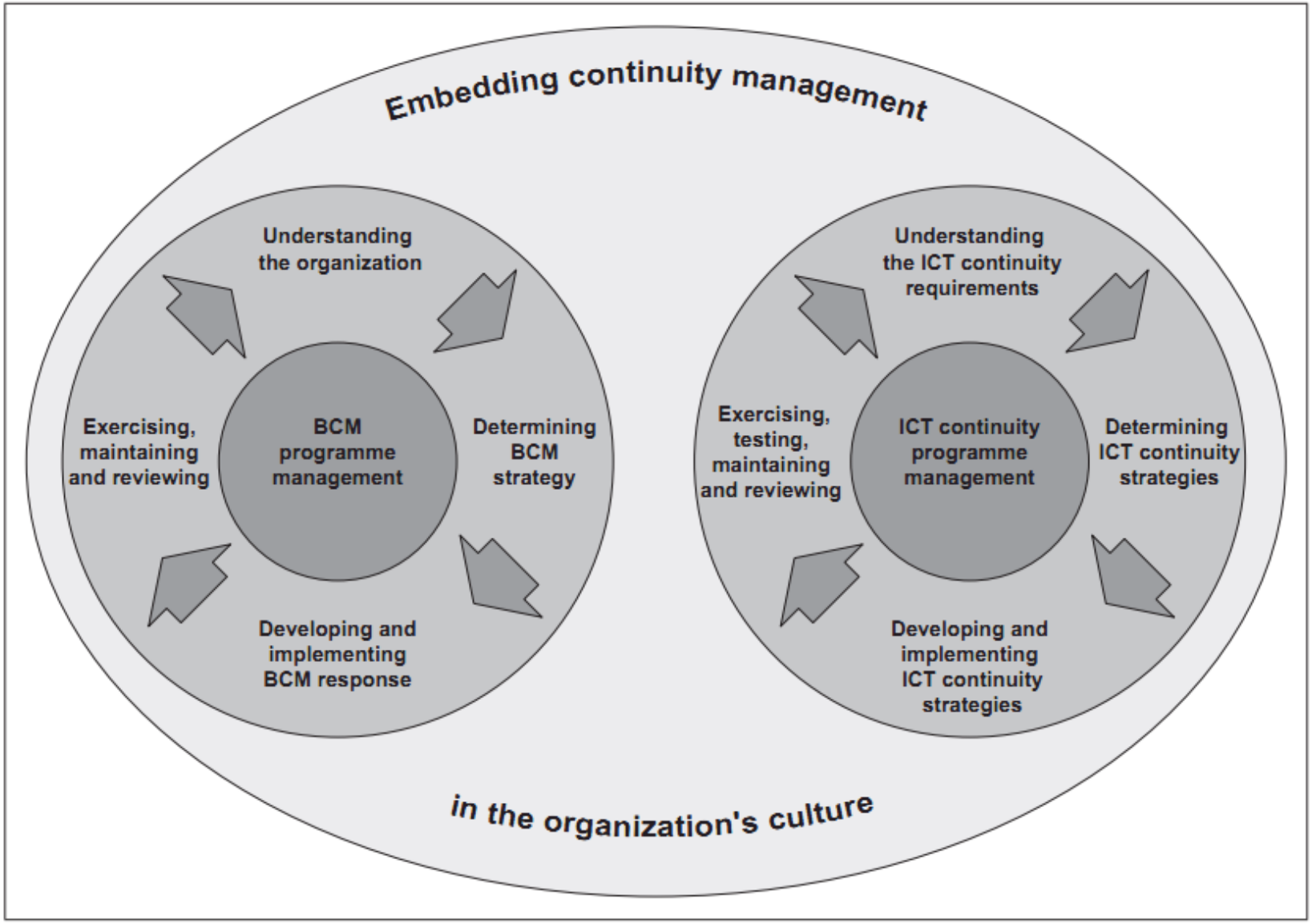
Was ist neu?

- Anwendung des PDCA-Zyklus



- Kapitel 8.4:
  - 8.4 Measurement of ICT Readiness Performance Criteria
  - 8.4.1 Monitoring and measurement of ICT Readiness
  - 8.4.2 Quantitative and Qualitative Performance Criteria

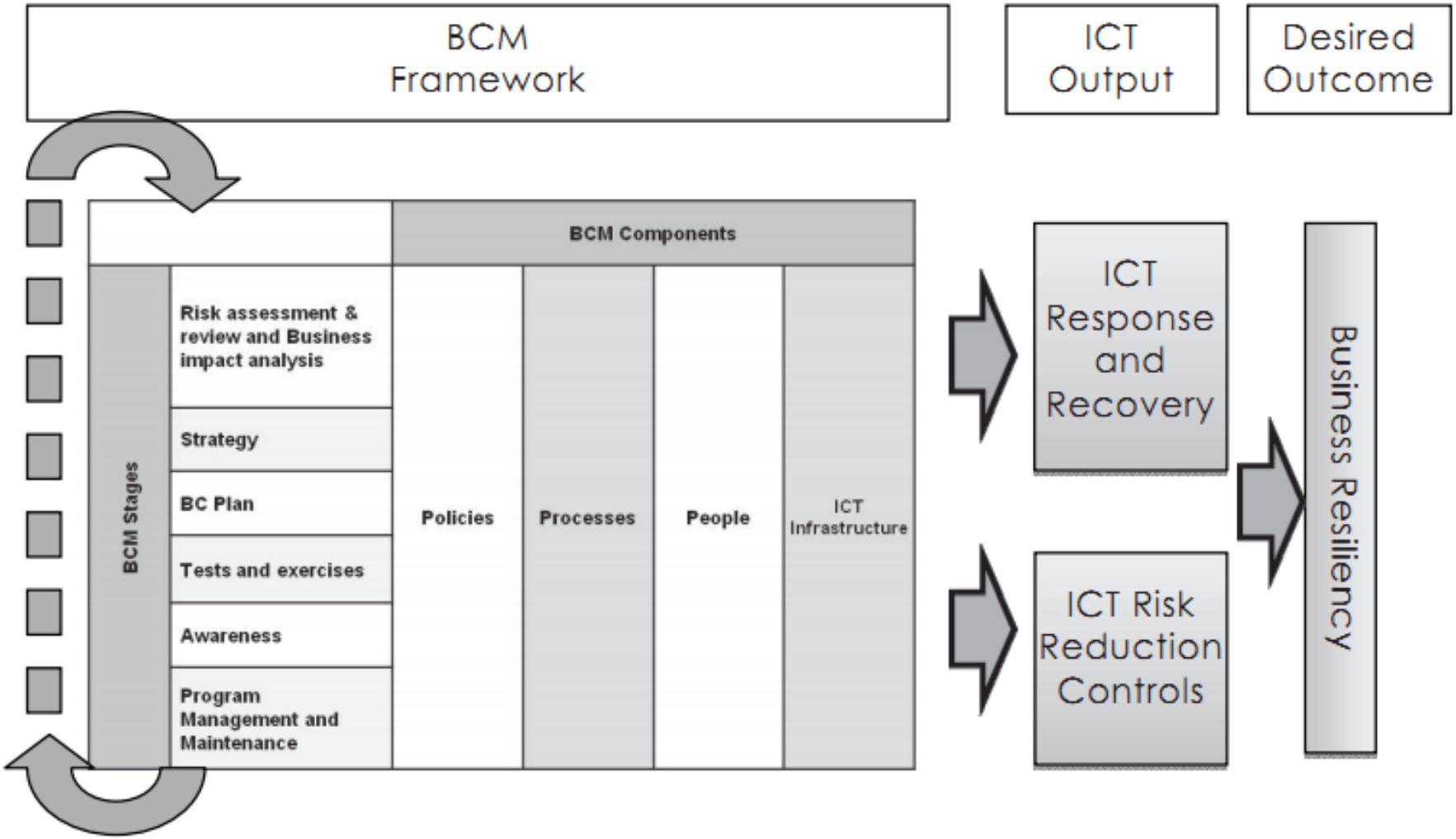
Besser im 25777



Anwendungsbereich

This International Standard describes the concepts and principles of **information and communication technology (ICT) readiness for business continuity**, and provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving an organization's ICT readiness to ensure business continuity.

ICT als Unterstützung für BCM



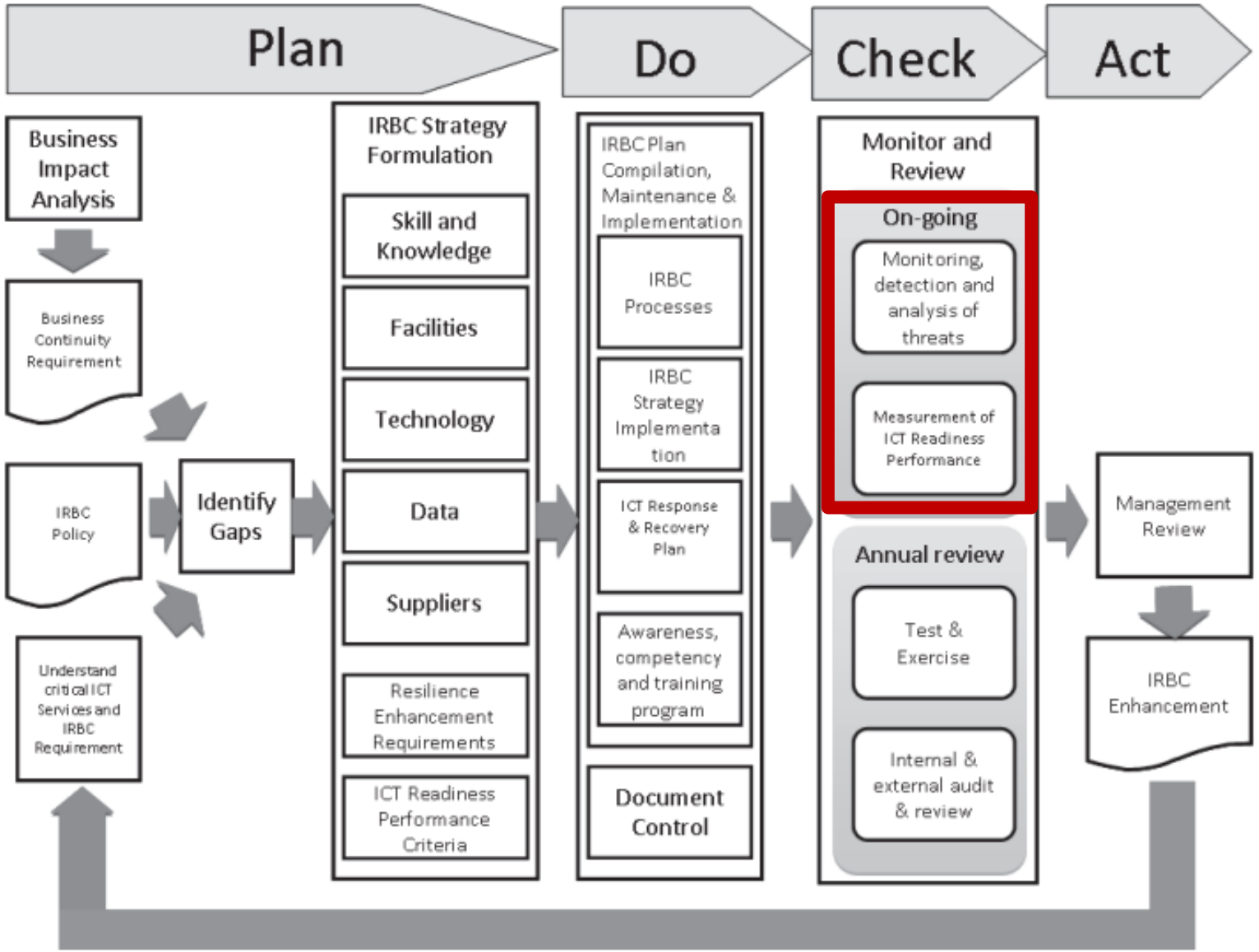
Dienstleister ?

ICT Readiness for Business Continuity

Elemente

- People
- Facilities
- Technology
  - Hardware
  - Network
  - Software
- Data
- **Processes**
- **Suppliers**

Neuer Teilaspekt



Nicht einverstanden mit

6.3.2 Understanding critical ICT services

…. The RTO of the critical ICT services will invariably be less than the business continuity RTO.

8.4 Measurement of ICT Readiness Performance Criteria

Quantitative criteria may include:

a) over a given period time, the **number of incidents that have not been detected prior to disruption** (this can provide an indication of the completeness of detection and alert mechanisms);

b) **detection time for incidents**;

c) **number of incidents** that cannot be effectively contained **to reduce impact**;

d) **availability of data sources** to indicate emergence of incidents through trend monitoring of events; and

e) **time to react and respon**d to detected emerging incidents.

8.4 Measurement of ICT Readiness Performance Criteria

Qualitative criteria may include determining the efficiency of the processes used in planning, preparing, and executing the activities of IRBC and can be measured through:

a) **survey** using structured or unstructured questionnaire;

b) **feedback** from participants and stakeholders;

c) conduct of **feedback workshops**; and

d) **other** focused **group meeting**.

Software Engineering Institute

CERT ® Resiliency Management Model, v1.0

Generic Goals and Practices

June 2009

Generic Goals and Practices

This document describes the generic goals and practices that the organization deploys to attain successively improving degrees of process institutionalization and **capability maturity for operational resiliency management**.

…

…

…generic goals and practices are applied universally across all process areas throughout the CERT Resiliency Management Model.

GG2.GP8 Monitor and Control the Process

… Monitoring and controlling the process involves **establishing appropriate metrics and measuring appropriate attributes** of the process or work products produced by the process.

…

Das hilft nicht!

ISO 27004

Information technology

Security techniques

Information security management

Measurement

Vorgehen übernehmen für BCM

This International Standard gives recommendations concerning the following activities as a basis for an organization to fulfil measurement requirements specified in ISO/IEC 27001:

a) **developing measures** (i.e. base measures, derived measures and indicators);
b) **implementing and operating** an Information Security Measurement Programme;
c) **collecting and analysing** data;
d) developing measurement **results**;
e) **communicating** developed measurement **results to** the relevant **stakeholders**;
f) **using** measurement **results** as contributing factors **to** ISMS-related **decisions**;
g) **using** measurement **results** to identify needs **for improving** the implemented ISMS, including its scope, policies, objectives, controls, processes and procedures; and
h) facilitating **continual improvemen**t of the Information Security Measurement Programme.

ISM ersetzen durch BCM

Wichtige Anmerkung für SMEs (KMUs)

For **SMEs** (Small and Medium Enterprises) **a less comprehensive** information security measurement **program will be sufficient**,

whereas **large enterprises** will implement and operate **multiple Information** Security Measurement Programmes.

A single Information Security Measurement Programme may be sufficient for small organizations, whereas for large enterprises the need may exist for multiple Information Security Measurement Programmes.

Messgrößen für das BCM

- übertragen aus Anhang
- übernommen, wenn sinnvoll für BCM
- ergänzt

Im Berichtszeitraum geschulte Notfallteams

Beispiel einer Messwertbeschreibung

Parameter	Erläuterung
Zielvorgabe	Prozentsatz der in der Notfallorganisation beteiligten Personen mit Stabs- und Leitungsfunktionen, die mindestens geschult sein müssen
Messwerte	Prozentsatz, (erfolgreich) geschulter Personen dividiert durch Personen gesamt
Datenquellen	Teilnehmerlisten der Schulungen Notfalldokumentation E-Schulungs-Tools
Messintervall	jährlich

Weitere Messwerte 1/2

- geschulte Notfallteams
- BCM-Schulungen
- geplante und durchgeführte externe Reviews
- durchgeführte Self-Assessments
- aufgetretene Notfälle
- durch Prävention verhinderte Notfälle
- BCM Maßnahmenverfolgung
  (geplant, durchgeführt, verschoben)
- Management-Beteiligung an BCM-Veranstaltungen
- Dienstleisterverträge mit BCM-Klauseln
- BCM-Audits bei Dienstleistern

Weitere Messwerte 2/2

- Anzahl erfolgreicher / nichterfolgreicher Tests (wichtig: Testvorgaben)
- relative Anzahl erfolgreicher Recovery von Einzelsystemen (Test und Notfall)
- Abdeckungsgrad kritischer Prozesse durch Tests
- Abdeckungsgrad Notfallszenarien durch Tests
- Aktualität der Notfallplanung bzgl. Veränderungen / Neuerungen
- Aktualität der Dokumentation
- Aktualität der BIA

Zusammenfassung

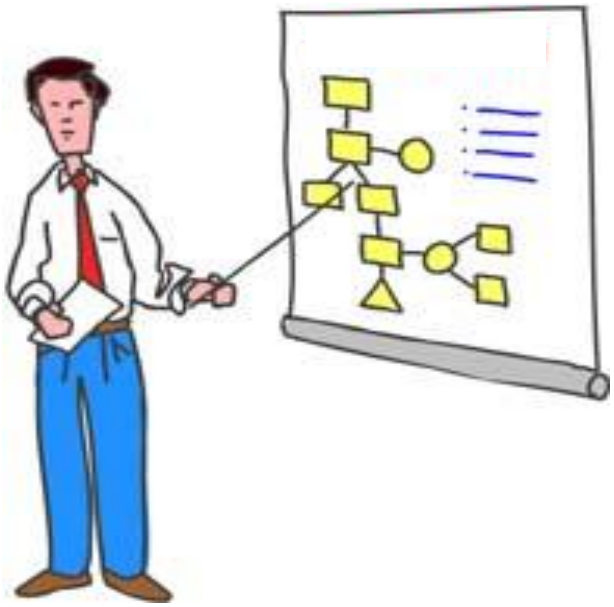
- Klein anfangen, später ggf. wachsen
- Berichtswesen Top-Down konzipieren
- Vorgaben mit Geschäftsleitung klären
- Einbetten in Kennzahlensystem des Unternehmens

Die schlimmsten Fehler werden nicht durch falsche Antworten verursacht.

Die größte Gefahr besteht darin, dass die falschen Fragen gestellt (Messwerte erhoben) werden.

nach Peter Drucker

Vielen Dank
für Ihre Aufmerksamkeit!



consequa

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