ICT readiness for business continuity – BCM und ISM wachsen zusammen

Know-how to go – ISO 27001 Novellierung

HiSolutions AG

Anton Lorenz

Anton Lorenz

Fachliche Schwerpunkte

- Beratung zu den Themen Business Continuity Management und Risk Management
- Umsetzung von Anforderungen aus dem BSI-Standard 200-4 und ISO 22301
- IT-Risikoanalysen nach BSI-Standard 200-3

Qualifikationen

- ISO 22301 – Lead Auditor (qSkills)
- zertifizierter BCM-Manager (TÜV Rheinland)
- ITIL 4 - Foundation Certificate IT Service Management
- BSI IT-Grundschutz Praktiker
- Master of Arts | Global Supply Chain and Operations Management

Agenda

1. Business Continuity in der ISO 27001
2. Business Continuity Management
3. BCMS und ISMS: Synergien nutzen
4. Wrap Up und Take Away

1. Business Continuity in der ISO 27001

Aktuell lassen die Anforderungen an das BCM viel Interpretationsspielraum

1. A.17 Informationssicherheitsaspekte beim Business Continuity Management
   a. A.17.1 Aufrechterhaltung der Informationssicherheit
      -> Berücksichtigung der Informationssicherheit im BCMS
   b. A.17.2 Redundanzen – Sicherstellung der Verfügbarkeit von informationsverartbeitenden Einrichtungen

➡ *Aktuell stehen die Anforderungen der Informationssicherheit allein im Zentrum der Überlegungen*

Neue Anforderung:
ICT readiness for business continuity

Sicherstellung der IKT-Verfügbarkeit auf Basis der Geschäftskontinuitätszielen und Anforderungen an die IT

Mit dem neuen Control werden die Kontinuitäts-Anforderungen geschärft

Umsetzungsmöglichkeiten aus der ISO 27002:

- Erforderliches Verfügbarkeitsniveau der IKT-Dienste auch während Störungen erreichen:

a) Aufbau und Implementierung einer Organisationsstruktur im Notfallmanagement
b) Business Impact Analyse (BIA) und Risikobewertung für (mind.) die IKT-Dienste
c) IKT- Kontinuitätsstrategien entwickeln
d) BC-Pläne erstellen, implementieren und testen

Verfügbarkeit der IKT sicherstellen

Verfügbarkeit der IKT sicherstellen

a) Anforderungen an die IKT bestimmen

b) Ausfallrisiken ermitteln und bewerten

c) Strategien und Maßnahmen zur Aufrechterhaltung entwickeln

d) Konkrete Pläne erstellen

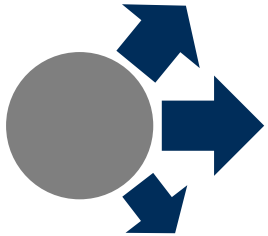
e) Üben und Testen der Pläne

RTO und RPO sollten bekannt sein

2. Business Continuity Management

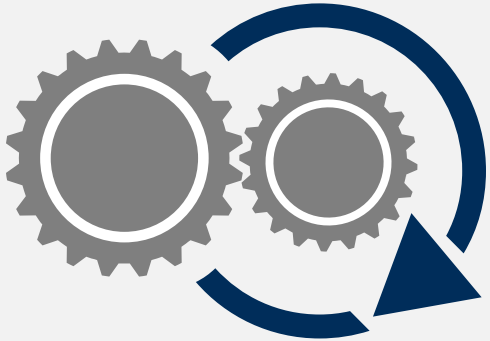
Ein vollständig wirksamer technischer Schutz ist heute nicht mehr erreichbar

144 Millionen neue Schadprogramm-Varianten (2020)



Stetig wechselnde Angriffsmethoden

Neben der **Prävention** gewinnt die **Erkennung** sowie der **richtige Umgang** mit erkannten Angriffen an Wichtigkeit



Business Continuity Management

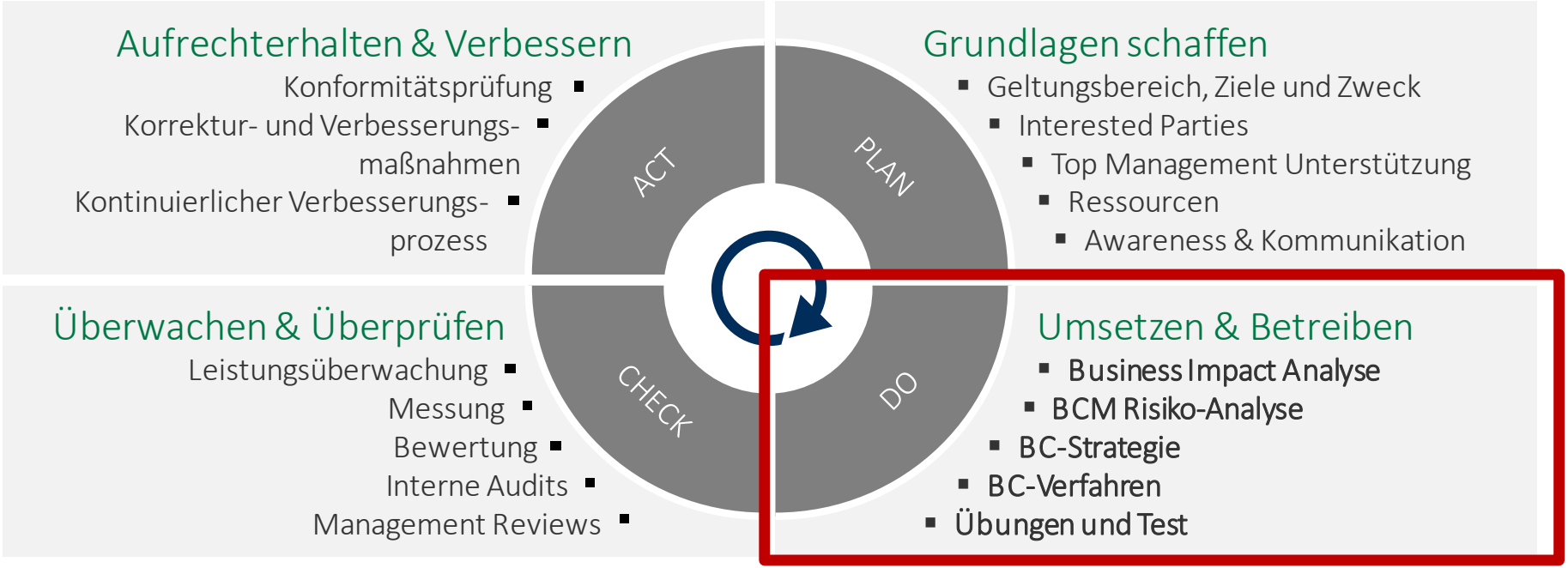
Ziel des BCM (deutsch: Notfallmanagement) ist es sicherzustellen, dass der Geschäftsbetrieb selbst bei massiven Schadensereignissen nicht unterbrochen wird (Prävention) oder nach einem Ausfall in angemessener Zeit fortgeführt werden kann (Reaktion).

BSI-Standard 200-4
Bundesamt für Sicherheit in der Informationstechnik

3. BCMS und ISMS: Synergien nutzen

Ein BCMS lässt sich gut in ein bestehendes ISMS integrieren

Der PDCA Zyklus des BCMS und des ISMS haben viele Schnittstellen

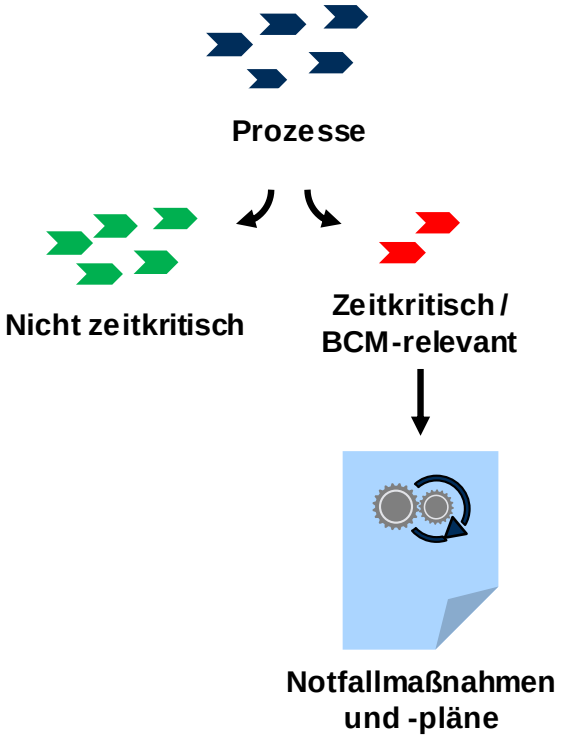


In der Business Impact Analyse werden zeitkritische Prozesse und Ressourcen sowie Abhängigkeiten identifiziert

Im Rahmen des Notfallmanagements sollen die vorhandenen Mittel zielgerichtet zur **Absicherung der zeitkritischen Prozesse und Ressourcen** eingesetzt werden.

Die **Business Impact Analyse (BIA)** ermittelt hierfür die zeitkritischen Prozesse, relevante Prozessabhängigkeiten sowie zur Durchführung der Prozesse notwendige Ressourcen (IT-Anwendungen, Dienstleister, Personal und Gebäude).

Die identifizierten zeitkritischen Prozesse und Ressourcen werden im Anschluss an die Business Impact Analyse durch Notfallmaßnahmen abgesichert.



Schnittstellen zwischen BIA, Strukturanalyse und Schutzbedarfsfeststellung

- Ergebnisse aus der Strukturanalyse/Prozesslandkarte als Datenbasis für die BIA (Identifizierung von Geschäftsprozessen und Ressourcen)
- Kombinierte Durchführung von Analysen wie SBF und BIA
  - Die selben Ansprechpersonen
  - Ähnliche Methoden bzw. aufeinander abgestimmte Methoden
  - Gemeinsame Datenerhebung

➢ **steigert die Akzeptanz in der Institution, reduziert Aufwände, vermeidet Widersprüche**

Gemeinsame Risiko-Analyse

- Kriterien und Methoden zur Risikobewertung aufeinander abstimmen
- Gleicher Betrachtungswinkel: Betrachtung von Ursachen eines Ausfalls des Geschäftsbetriebs oder einzelner Ressourcen
- Gleiche Gefährdungen als Ausgangsbild (z.B. elementare G0-Gefährdungen des BSI)
- Gemeinsame Übersicht der relevanten Risiken, um einen umfassenden Blick auf die notwendigen Sicherheits- und BC-Lösungen zu erhalten

➢ **Integrierter Risikobehandlungsplan, um finanzielle, personelle und zeitliche Ressourcen z.B. durch Synergieeffekte einzusparen**

BC-Strategien

Identifikation möglicher Strategien

…bspw. anhand der vier klassischen Ausfallszenarien

Gebäude und Infrastruktur

IT-Anwendungen und -Services

Dienstleistungen

Personal

BC-Verfahren zur Notfallbewältigung

Die richtigen Pläne und Personen

Merkmale eines effizienten Notfallplans

Vollständigkeit

- Korrekten Verwendung der Hilfsmittel zum GFP
- Abbildung aller notwendiger Inhalte
- Erfassung aller Inhalte aus der BIA
- Beschreibung sämtlicher Notfallmaßnahmen über alle Phasen

Plausibilität

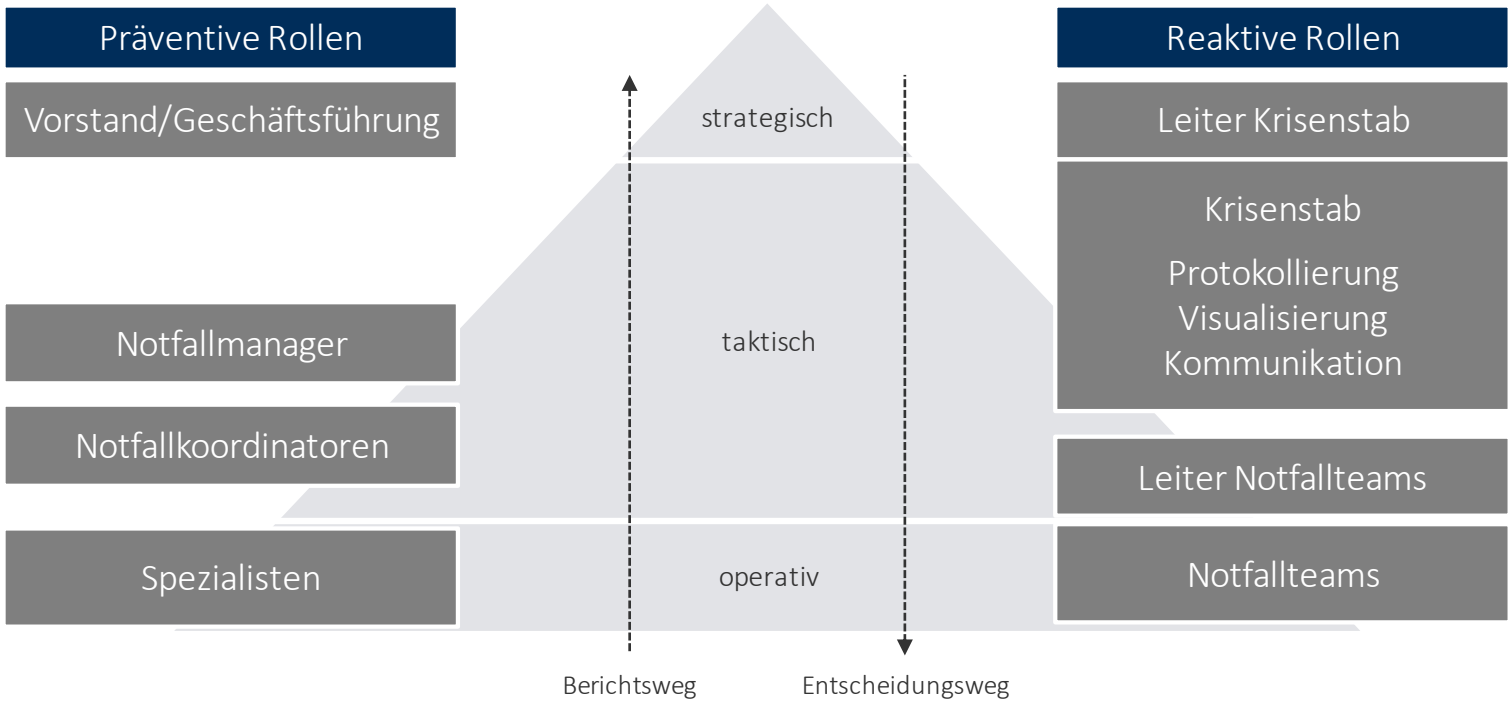
- Eignung der Notfallmaßnahmen zur Überbrücken der Wiederanlaufzeit und zur Erreichung des Notbetriebsniveau
- Widerspruchsfreiheit der Maßnahmen

Aktualität

- Version der referenzierten Dokumente
- Aktualität der Kontaktliste der Ansprechpartner

Ziel: Einheitliche und nachvollziehbare Dokumentation zur schnellen Anwendbarkeit

Organisationsstruktur im BCM



Übung macht den Meister

Sammeln von Erfahrungen im Umgang mit realistischen Szenarien in einer geschützten Umgebung

Übersicht aktueller Standards

ISO 22301:2019

Internationaler Standard

Anpassung des Aufbaus an übrige ISO Normen

ISO 22313:2020

Umsetzungsempfehlung der ISO 22301

Tipps und Anweisungen

ISO 22317:2021

Implementierung und Durchführung der BIA

ISO 27031:2011

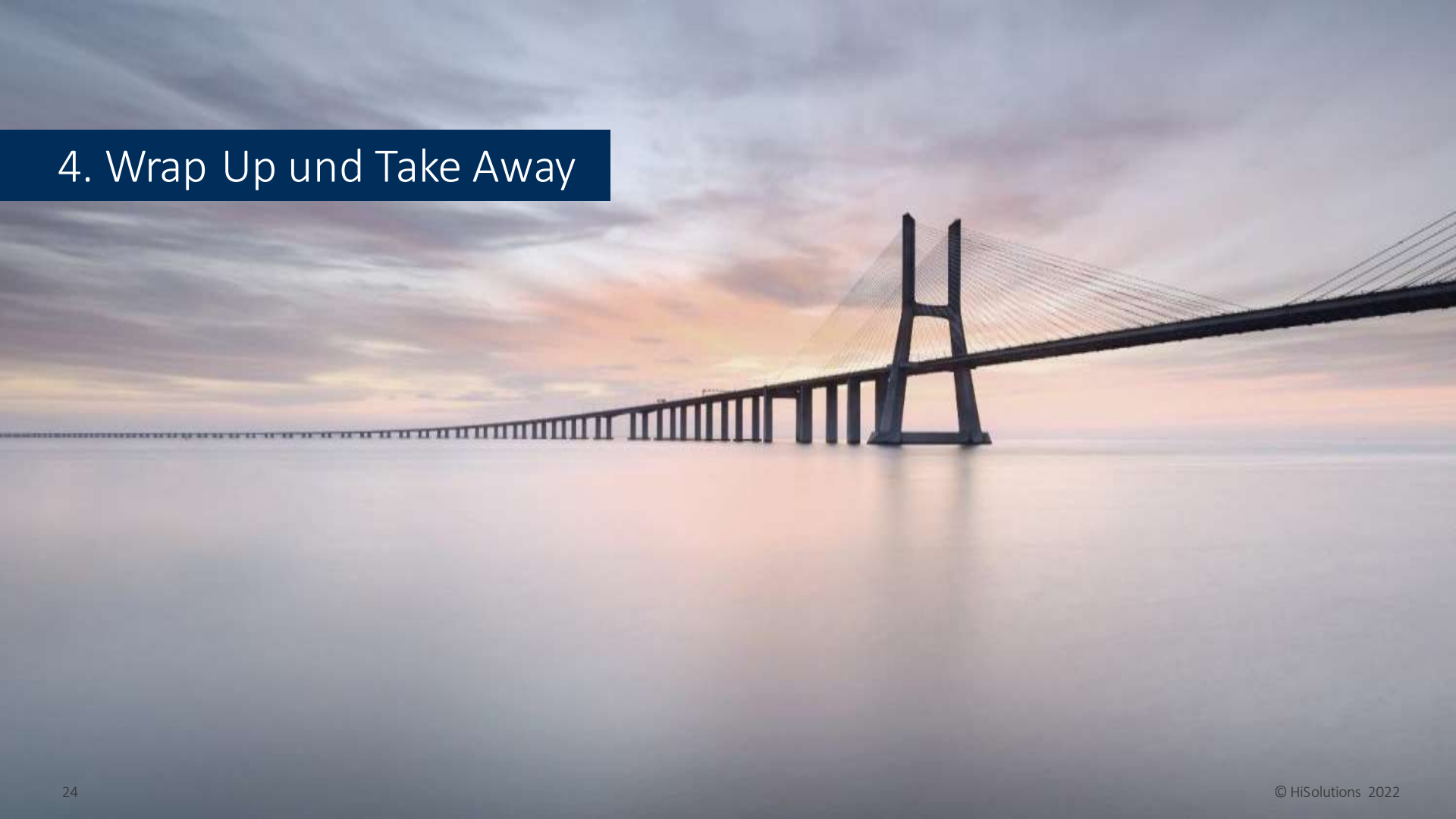
Fokus auf ITSCM

BSI 200-4

Gesamtkonzept

Der aktuell allumfassendste BCM-Standard im deutschsprachigen Raum

4. Wrap Up und Take Away

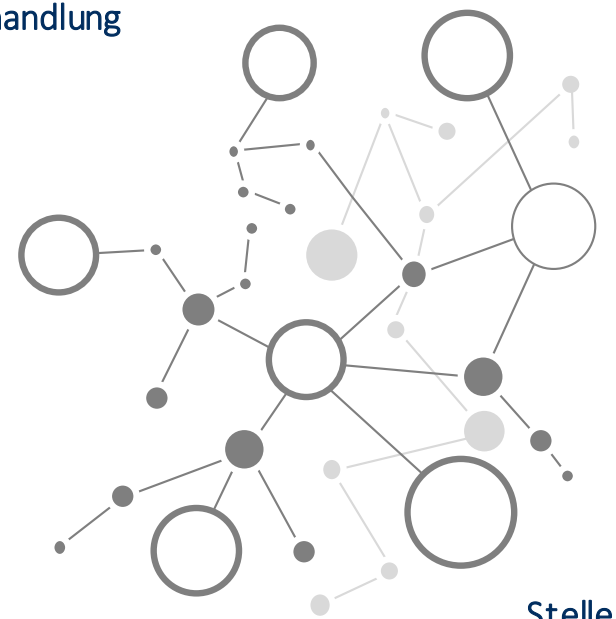


Wesentliche Schnittstellen im Überblick

Risiko-Analyse und -Behandlung

Umsetzungsmaßnahmen

Notfallbewältigung



Strukturanalyse,
Schutzbedarfsfeststellung und
Business Impact Analyse

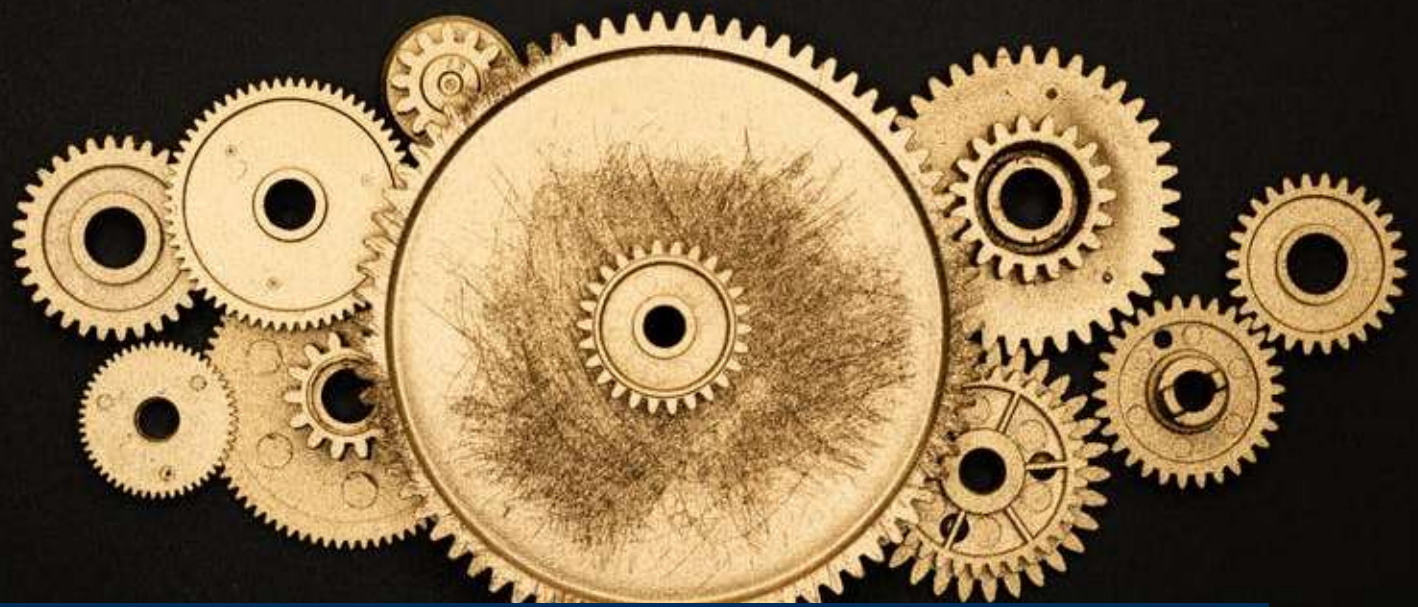
Informationsfluss

Stellenbesetzung

Anforderungen zum BCM wurden konkretisiert und verschärft

- Wer ein bestehendes BCMS hat, ist auf der sicheren Seite
- Auch mit einem ITSCM sollten die Anforderungen erfüllt werden können
- Einhaltung der Anforderungen durch Integration der Schritte in das bestehende ISMS

- Kontinuitätsziele kennen
- IKT muss auch im Schadensfall abgesichert sein und die geforderten Verfügbarkeiten gewährleistet werden
  - Dafür müssen die Anforderungen bekannt sein
  - Nur gelebte Pläne können auch die Verfügbarkeit gewährleisten -> regelmäßiges Üben und Testen, um die Funktionalität zu überprüfen



Das Zusammenspiel der beiden Managementsysteme steigert die Resilienz des Unternehmens

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com