Business Continuity

Mapping von Risiken und Szenarien

05.10.2023, Impulsvortrag

IHK Südlicher Oberrhein

SDCON

Wer ist SD-Con?

Kurzvorstellung

IHK Südlicher Oberrhein

SDCON

Wer sind wir?

- Beratungsunternehmen, gegründet 2009
- Mitarbeiter: 7
- Büros:
  87600 Kaufbeuren
  36325 Feldatal
- Aktive Kunden: ca. 130 in D/A/CH, branchenübergreifend

Was können wir?

- Integrierte Managementsysteme (IMS)
- Methoden, Prozesse, Audits, Schulungen
- Compliance- und Nachhaltigkeits-Management
- Maßnahmenorientierte Organisation
- Betrieb eines Kunden- und Wissensportals

Orga und Agenda

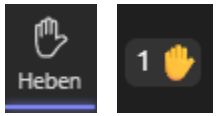
Worum geht es heute?

IHK Südlicher Oberrhein

SDCON

Wie gehen wir heute miteinander um?

Kamera und Mikro standardmäßig deaktivieren !
Tippen mit offenem Mikro stört die anderen, die Kamera beeinträchtigt u.U. die Bandbreite bei vielen Teilnehmern…



Diskussion erwünscht !
Einfach Hand heben, die Moderatoren passen hoffentlich auf…

Chatten !
Einfach Dinge in den Chat schreiben, die Moderatoren passen hoffentlich auf …

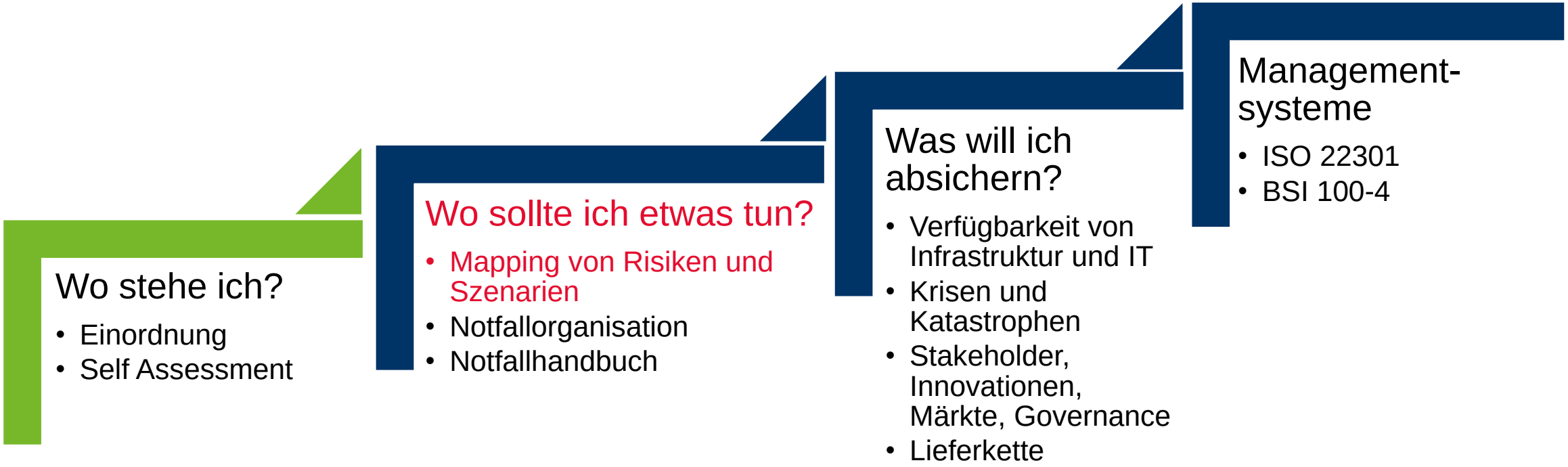
Zielsetzungen Vortragsreihe

Überblick geben:
Was nützt Continuity Management?

Orientierung geben:
Was kann ich tun?
Wieviel sollte ich tun?

Tools an die Hand geben:
Nützliche Hilfsmittel, einfaches Notfall-Handbuch, Tools für ein Managementsystem

Verankerung in der Organisation:
Organigramm , Prozesse, Verfahrensanweisungen, Dokumente


Wo stehe ich?
• Einordnung
• Self Assessment
Wo sollte ich etwas tun?
• Mapping von Risiken und Szenarien
• Notfallorganisation
• Notfallhandbuch
Was will ich absichern?
• Verfügbarkeit von Infrastruktur und IT
• Krisen und Katastrophen
• Stakeholder, Innovationen, Märkte, Governance
• Lieferkette
Management-systeme
• ISO 22301
• BSI 100-4

Agenda für heute

- **Rückblick: Self Assessment**
- **Mapping Risiken und Szenarien**
  - Was ist eine Business Impact Analyse (BIA)?
  - BIA und Risikoanalyse
  - Maximal tolerierbare Ausfallzeit
  - BIA „light“: Inventarliste, Prozessliste, Zusammenführung im Assessment
- **Ausblick auf Notfallorganisation und Notfallhandbuch**

Warum Business Continuity Management?

Was sind Ihre Erwartungen für heute?

Rückblick

Self-Assessment

IHK Südlicher Oberrhein

SDCON

Was ist ein Assessment?

- **Einschätzung bzw. Bewertung gegen festgelegte Anforderungen**
- **Einsatz z.B. in den Bereichen Personalmanagement, Bewertung von Wissen/Kompetenzen,**
  Erfüllung von Managementsystem-Anforderungen, Einschätzung von Patienten zum Gesundheitszustand
- **Aspekte**
  - Klärung der relevanten Anforderungen für das Assessment
  - Einschätzung des Erfüllungsgrad der Anforderung
  - Abgrenzung gegen eine gewünschte Zielgröße
  - Ableitung eines Deltas bzw. von Handlungsbedarf

Self-Assessment

Rufen Sie unser Self Assessment „Business Continuity“ auf !

Die Adresse übertragen wir in den Chat:
https://service.sd-con.de/containerDocs/CE0A28BA

Nach Eingabe der Mailadresse:

- **Müssen Sie sich zunächst registrieren, sofern noch nicht bekannt**
- **Können Sie danach die Datei herunterladen**
- **Der Abruf erfolgt gegen eine TAN, die Ihnen bei Bedarf an die hinterlegte Mailadresse zugesendet wird**

Wie wird die Bewertung durchgeführt?

- **Auswahl der relevanten Maßnahmen/Themen**
  - Festlegen/Aktivieren der bewertungsrelevanten Maßnahmen/Themen
  - Filtern auf relevante Maßnahmen/Themen
- **Bewertung 1-10:**
  - Wichtigkeit der Erfüllung
  - Eigene Fähigkeit zur Erfüllung
  - Delta: Handlungsbedarf
- **Bewertung des Handlungsbedarfs: Ist eine Aktion notwendig?**

Maßnahme	Relevanz zur Bewertung	Wichtigkeit der Erfüllung	Eigene Fähigkeit	Handlungs-bedarf
Absatzsicherheit erreichen	X	5	7	-2
Änderungen berücksichtigen				0
Anlagensicherheit gewährleisten	X	7	4	3
Anschläge überstehen				0
Anwendungsbereich des Systems festlegen				0
Auditoren qualifizieren				0
Beauftragte/n einsetzen				0
Bedienfehler kompensieren				0
Betrieb aufrechterhalten	X	9	7	2
Betrugsdelikte vermeiden/abwickeln	X	3	3	0
Bewusstsein fördern				0
Brände überstehen	X	9		9
Business Continuity verbessern				0
Business Impact Analyse durchführen				0
Compliance Management umsetzen				0
Compliance-Anforderungen erfassen	X	5		5
Cyberangriffe abwehren	X	7		7

Haben Sie sich das Assessment angeschaut und Handlungsbedarf erkannt?
Wie setze ich den Handlungsbedarf um?

Mapping Risiken und Szenarien

IHK Südlicher Oberrhein

SDCON

Was ist eine Business Impact Analyse?

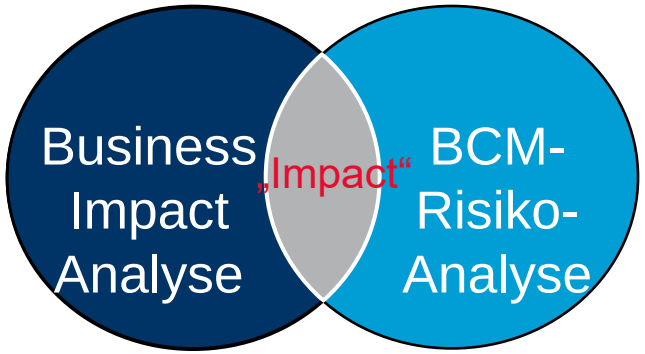
- **Eine Business Impact Analyse dient der Identifikation von Störungen, die eine Auswirkungen auf Geschäftsprozesse haben (können). Prozesse werden bewertet in Bezug auf**
  - Risiken
  - Ausfallzeit und Schadenwirkung
  - Bewertung von Systemen / Infrastruktur zur Bereitstellung des Prozesses
  - Bewertung von personellen Ressourcen zur Bereitstellung des Prozesses
- Die Business Impact Analyse ist Bestandteile eines BCM-Systems nach ISO 22301. Wir beschränken uns zunächst auf eine „BIA light“

BIA und Risikoanalyse:

Was muss abgesichert werden?

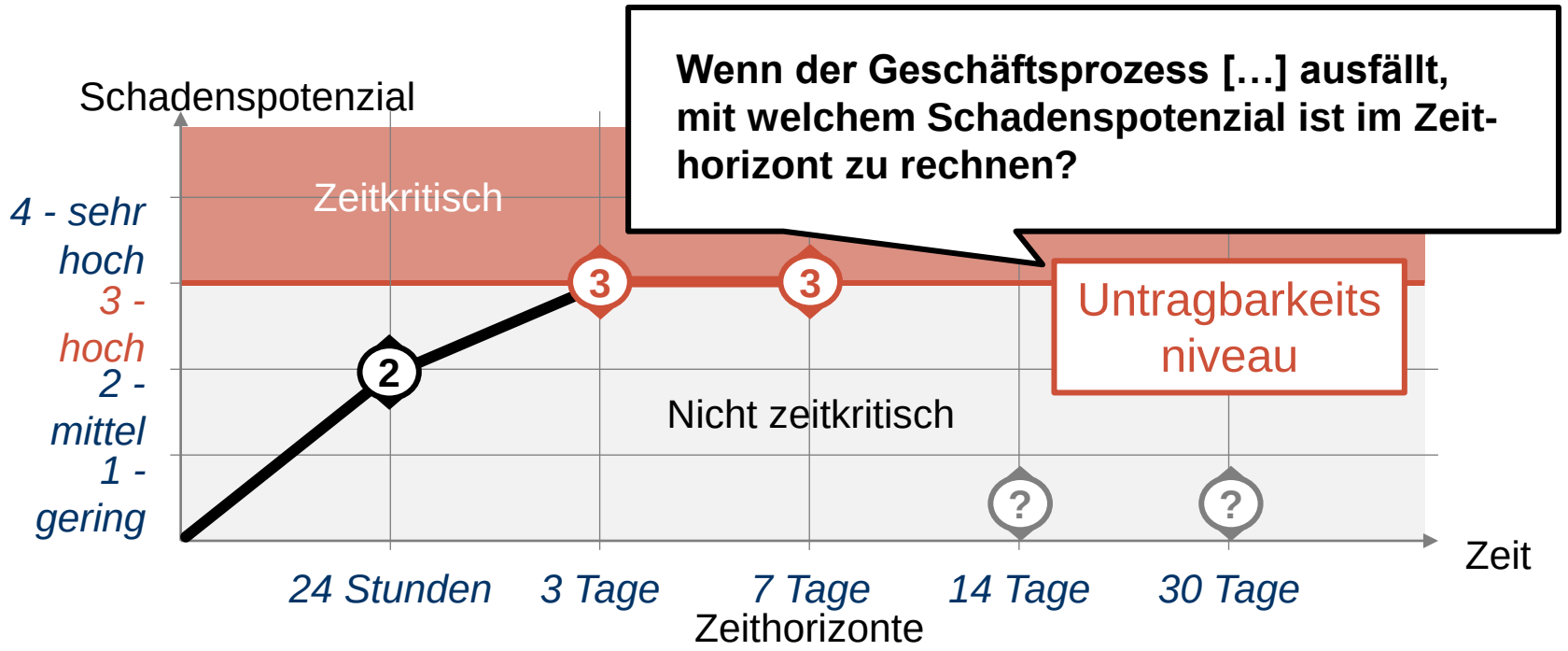
Wogegen muss abgesichert werden?

- Prozessbezogen
- Wirkungsorientiert
- Blendet vorhandene Maßnahmen aus (worst case)
- Ergebnis: Zeitwert (MTPD/RTO/RPO)



- Ressourcenbezogen
- Ursachenorientiert
- Berücksichtigt vorhandene Risiko-reduzierende Maßnahmen
- Ergebnis: Risikowert

Maximal tolerierbare Ausfallzeit: Zeithorizont und Schadenspotenzial



Warum eine BIA „light“?

- **Wir beschränken uns in dieser Phase des Notfallmanagements auf eine einfache Betrachtung des Inventars und vorhandener Prozesse:**
  - Einfache Ausfallbewertung (keine Zeit-/Schaden-Matrix)
  - Inventar wird erfasst, bewertet und mit Maßnahmen des Assessments verknüpft
  - Prozesse werden erfasst, bewertet und mit Maßnahmen des Assessments verknüpft
  - Im Assessment wird aufsummiert, wie viele Inventar– und Prozessbezüge vorhanden sind
- WICHTIG: Der Fokus liegt darauf, zu erkennen, ob für alle relevanten Maßnahmen Prozess- und Inventarbezüge vorhanden sind bzw. wo Lücken bestehen

BIA “light”

Rufen Sie unsere Dokumente auf!

- **ZIP-Datei mit 3 Excel-Dateien (Assessment und BIA „light“, Inventarliste, Prozessliste BCM): https://service.sd-con.de/containerDocs/F04A9D75**

Nach Eingabe der Mailadresse:

- **Sie müssen sich registrieren, sofern die Mailadresse uns noch nicht bekannt ist**
- **Danach können sie die Datei herunterladen.**
  Der Abruf erfolgt gegen eine TAN, die an die hinterlegte Mailadresse gesendet wird

Inventarliste

- **Die Inventarliste setzt auf vorhandenen Inventaren (Gebäude, Infrastruktur, Equipment) auf. Das Inventar wird bewertet nach**
  - Unternehmensbereich
  - Risiko
  - Maßnahmenbezug
  - Reaktionszeit / Schadenauswirkung
  - Ergriffenen Aktionen zur Risiko- und Schadenminderung
  - Restrisiko

Unternehmensbereich	Anlagen	Risiko	Bezug zu Maßnahme	tolerierb. Zeit	Schadenauswirkun	Ergriffene Aktionen	Restrisik
IT	Archivsystem / Dokumentenmanagement	Ausfall	IT- und Kommunikationsausfälle kompensieren	sehr kurz (Stunden)	hoch	Virtualisierung und	1
IT	Backup-Infrastruktur	Fehlerhafte Backups	IT- und Kommunikationsausfälle kompensieren	mittel (2-3 Tage)	gering	Restore-Tests	1
IT	CRM-System	Ausfall	Betrieb aufrechterhalten	kurz (1 Tag)	mittel	Virtualisierung und	3
IT	ERP-System / Warenwirtschaft	Ausfall	IT- und Kommunikationsausfälle kompensieren	sehr kurz (Stunden)	hoch	Virtualisierung und	1
IT	ERP-System / Warenwirtschaft	Ausfall	Betrieb aufrechterhalten	sehr kurz (Stunden)	sehr hoch	Virtualisierung und	5
IT	Kommunikations-Infrastruktur	Ausfall	IT- und Kommunikationsausfälle kompensieren	sehr kurz (Stunden)	sehr hoch	Ausfallsicherheit und	3
IT	Netzwerk-Infrastruktur	Ausfall	IT- und Kommunikationsausfälle kompensieren	sehr kurz (Stunden)	hoch	USV	1
IT	Notstromanlage Instandhaltung, EDV	Ausfall	IT- und Kommunikationsausfälle kompensieren	kurz (1 Tag)	mittel		1
IT	Serverraum	Ausfall	IT- und Kommunikationsausfälle kompensieren	sehr kurz (Stunden)	sehr hoch	Hardware-Absicherung	1
IT	Server lokal	Ausfall	IT- und Kommunikationsausfälle kompensieren	sehr kurz (Stunden)	sehr hoch	Virtualisierung und	1
IT	Server Cloud/RZ	Ausfall	IT- und Kommunikationsausfälle kompensieren	sehr kurz (Stunden)	sehr hoch	Virtualisierung und	1
IT	USV	Ausfall	IT- und Kommunikationsausfälle kompensieren	kurz (1 Tag)	mittel		
IT	IT-Security Maßnahmen (Viren, Firewall, ...)	Ausfall	IT- und Kommunikationsausfälle kompensieren	sehr kurz (Stunden)	sehr hoch	Virenschutz abgestuft, Patch	1

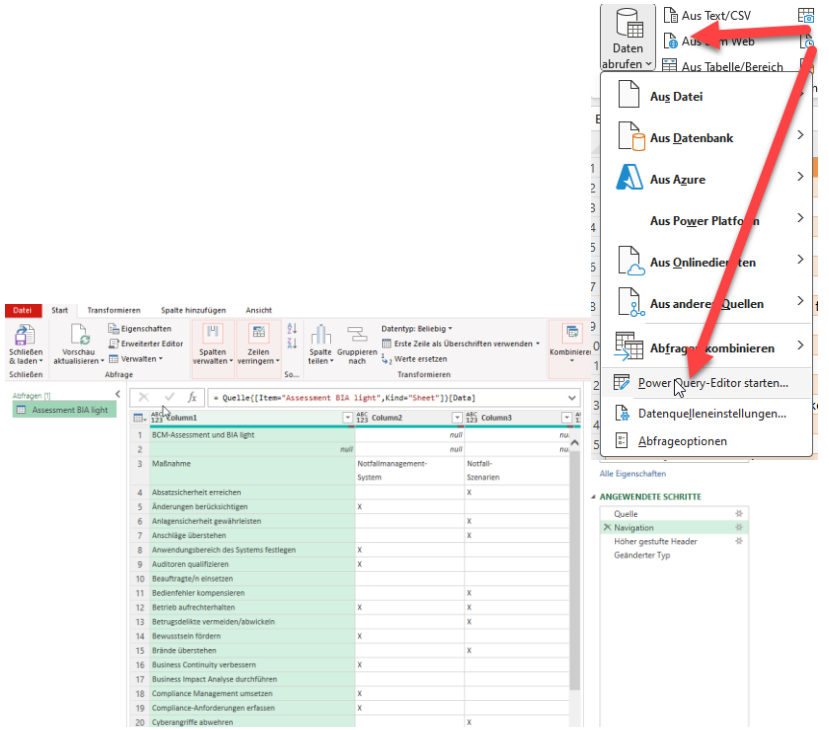
Prozessliste

- **Die Prozessliste setzt auf vorhandenen Prozessen / Prozessbeschreibungen auf. Prozesse werden bewertet nach**
  - Unternehmensbereich
  - Risiko
  - Maßnahmenbezug
  - Reaktionszeit / Schadenauswirkung
  - Ergriffenen Aktionen zur Risiko- und Schadenminderung
  - Restrisiko

Unternehmens-bereich	Prozess/ Dokument	Teilprozess	Risiko	Bezug zu Maßnahme	tolerierb. Zeit	Schadenaus wirkung	Ergriffene Aktionen	Restrisiko
IT	Ressourcen Allgemein	IT-Sicherheit erhöhen	Fehlbewertung	IT- und Kommunikationsausfälle kompensieren	kurz (1 Tag)	hoch		
IT	Ressourcen Allgemein	IT-Sicherheit erhöhen	Fehlendes Budget	IT- und Kommunikationsausfälle kompensieren	lange (4-5 Tage)	mittel	Prozess regelmäßig prüfen, priorisieren	1
IT	Prozesse IT	IT-Infrastruktur planen und bereitstellen	Performanceprobleme	Ressourcen bestimmen und überwachen	lange (4-5 Tage)	gering	Monitoring und Virtualisierung	1
IT	Prozesse IT	IT-Anwendungen bereitstellen	Verfügbarkeit	IT- und Kommunikationsausfälle kompensieren	kurz (1 Tag)	mittel	Monitoring und Virtualisierung	1
IT	Prozesse IT	IT Change Management	Alte SW	IT- und Kommunikationsausfälle kompensieren	lange (4-5 Tage)	gering	Asset-Management und IT-Strategie	1
IT	Prozesse IT	IT Security Management	Hacking, Viren	Cyberangriffe abwehren	sehr kurz (Stunden)	mittel	Security-Software, Patch-Management, Ui	1
IT	Prozesse IT	Monitoring	Performanceprobleme	Ressourcen bestimmen und überwachen	sehr kurz (Stunden)	mittel	Asset-Management und Monitoring	1
IT	Prozesse IT	Ticketing	Ausfall	IT- und Kommunikationsausfälle kompensieren	sehr kurz (Stunden)	mittel	Asset-Management und Monitoring	1
IT	Prozesse IT	Backup/Restore	Fehlerhafte Backups	IT- und Kommunikationsausfälle kompensieren	sehr kurz (Stunden)	mittel	Übungen	1

Tabellenverknüpfungen in Excel

- **Daten werden aus anderen Dateien/Tabellen per Power Query Editor abgefragt**
  - Prüfen Sie ggf. die jeweilige Quelldatei
  - Prüfen Sie ggf. das Register
  - Prüfen Sie ggf. die Tabelle



BIA “light”

Wer hat Interesse an einer einfachen Excel-Datei?

- Bei Bedarf erzeuge ich eine einfache Excel-Datei, in der alle Tabellen ohne Power Query enthalten sind
- E-Mail an t.schweppe@sd-con.de

Zusammenführung in Assessment / BIA „light“

- **Die Maßnahmen des Assessments mit ihrer Relevanzbewertung werden ergänzt um Anzahl Inventare und Anzahl Prozesse mit Bezug auf die jeweilige Maßnahme**
- **Nutzen**
  - Erkennung von Maßnahmen mit Handlungsbedarf, zu denen es keine Inventarbezüge und/oder Prozessbezüge gibt
    -> Handlungslücken
  - Erkennung von Inventaren und Prozessen, welche einen Maßnahmenbezug haben, die jedoch nicht im Assessment berücksichtigt wurden
    -> Konsistenzlücken

BCM-Assessment und BIA "light"

Maßnahme	Relevanz zur Bewertung	Wichtigkeit der Erfüllung	Eigene Fähigkeit	Handlungs-bedarf	Anzahl Inventar	Anzahl Prozesse
Absatzsicherheit erreichen	X	5	7	-2		
Anlagensicherheit gewährleisten	X	7	4	3		
Anschläge überstehen						
Bedienfehler kompensieren						
Betrieb aufrechterhalten	X	9	7	2	16	3
Betrugsdelikte vermeiden/abwickeln	X	3	3			
Brände überstehen	X	9		9		
Cyberangriffe abwehren	X	7	8	-1	2	1
Datenschutzverletzungen vermeiden	X	9	9			

Weiterführende Möglichkeiten und Ausblick

- **Die einfache Referenzauswertung könnte um zusätzliche Informationen erweitert werden**
  - Auswertung des Restrisikos je Maßnahme mit Durchschnitt / Median / Standardabweichung
  - Auswertung nach tolerierbaren Zeiten über Maßnahmen und Unternehmensbereiche
  - Auswertung nach Schadensauswirkungen über Maßnahmen und Unternehmensbereiche
  - Pflege der Risiken in eigener Datei als „Risikokatalog“,
    Auswertung der Risiken nach Maßnahmen und Bereichen
- **Portal-App „Maßnahmen-Container“**
  - Wir entwickeln derzeit einen Maßnahmen-Container in unserem Serviceportal
  - Ziel: Bewertung kundenspezifischer Maßnahmensammlungen gegen Normanforderungen, Prozesse, Dokumente, Gesetze, Inventare

BIA “light”

Was sind die Erkenntnisse?

- **Assessment:**
  Bewertung von zu erfüllenden Maßnahmen zur Business Continuity, Ableitung von Handlungsbedarf
- **Inventarliste:**
  Welches Inventar in welchen Unternehmensbereichen hat Risiken?
- **Prozessliste:**
  Welche Prozesse in welchen Unternehmensbereichen haben Risiken?
- **Zusammenführung in BIA „light“:**
  Passt der „gefühlte“ Handlungsbedarf zu Inventarrisiken und Prozessrisiken?
- **Ausrichtung des Notfallhandbuchs auf die Erkenntnisse der BIA „light“**

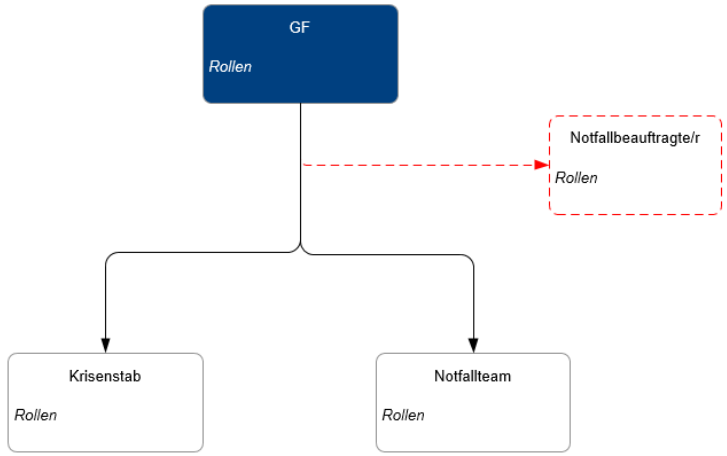
Ausblick auf Notfallorganisation und Notfallhandbuch

IHK Südlicher Oberrhein

SDCON

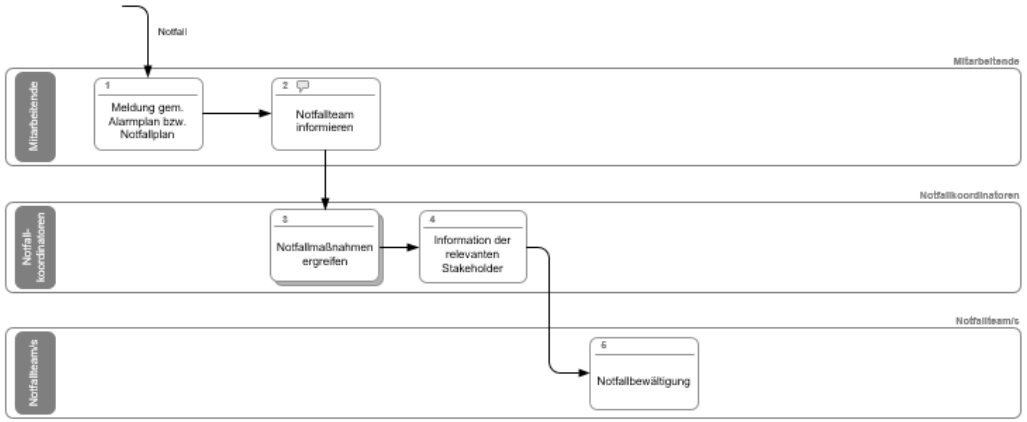
Abbildung der Notfall-Organisation

- **Unternehmensleitung:**
  - Sicherstellung des Notfallmanagement
  - Festlegung der Bedeutung des Notfallmanagements, stellt finanzielle und personelle Ressourcen zur Verfügung.
  - Ernennt den Notfallbeauftragten mit der Planung und Koordinierung aller Aufgaben im Rahmen des Notfallmanagement-Prozesses.
- **Notfallbeauftragte/r:**
  - steuert alle Aktivitäten rund um die Notfallvorsorge
  - Ist zuständig für Erstellung, Umsetzung, Pflege und Betreuung des Notfallmanagements und der zugehörigen Dokumente und Regelungen.
- **Krisenstab:**
  - Temporäres Führungsgremium zur Bewältigung von Notfällen
  - plant, koordiniert, informiert, berät, unterstützt
- **Notfallteam/s:**
  - Operative Notfallbewältigung
  - Zuständig für Wiederanlauf und Wiederherstellung



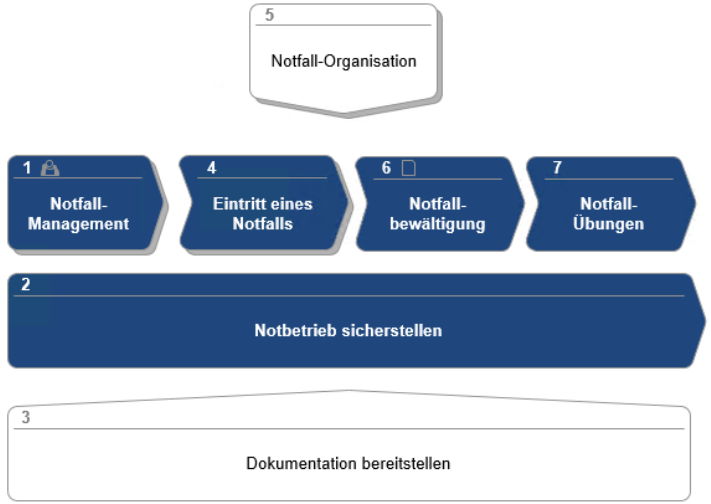
Eintritt eines Notfalls

- **Phasen:**
  - Eintritt eines Notfalls mit Meldung
  - Bewertung der Lage und Auswirkungen
  - Eskalation, Ergreifen von Sofortmaßnahmen
  - Initiierung von Wiederanlauf und Wiederherstellung, ggf. Bereitstellung eines Notbetriebs
  - Notfallnachsorge und Nacharbeiten
- **Ziele:**
  - Schnelligkeit und Angemessenheit
  - Transparenz und schneller Zugriff auf die wichtigen Informationen für alle Beteiligten



Das Notfall-Handbuch

- **Gesamtheit aller für die Notfallbewältigung benötigter Prozesse, Dokumente, Strukturen, Informationen sowie der erforderlichen Maßnahmen und Aktionen nach Eintritt eines Notfalles**
  - Erstellung im Vorfeld zu einem Notfall in Verbindung mit einem Notfallvorsorgekonzept
  - Zweck: Hilfestellung zur Bewältigung von Krisen und Notfällen mit einfachen und schnellen Handlungsanweisungen
- **Wesentliche Teile**
  - Plan für die Sofortmaßnahmen
  - Krisenstabsleitfaden
  - Krisenkommunikationsplan
  - Geschäftsfortführungspläne
  - Wiederanlaufpläne.



Und was jetzt?

Fragen bitte an:

Thomas Schweppe
t.schweppe@sd-con.de