Business Continuity

Szenario – IT-Verfügbarkeit

07.03.2024, Impulsvortrag

IHK Südlicher Oberrhein

SDCON

Wer ist SD-Con?

Kurzvorstellung

IHK Südlicher Oberrhein

SDCON

Wer sind wir und was tun wir?

- **Das Unternehmen**
  - 2009 gegründet, 7 Mitarbeiter
  - Büros in
    36325 Feldatal
    87600 Kaufbeuren
  - Ca. 130 aktive Kunden in D/A/CH, branchenübergreifend
- **Beratungsthemen**
  - Integrierte Managementsysteme (IMS)
  - Methoden, Prozesse, Audits, Schulungen
  - Compliance- und Nachhaltigkeits-Management
  - Regelbasierte Organisation

Orga und Agenda

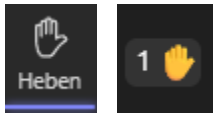
Worum geht es heute?

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

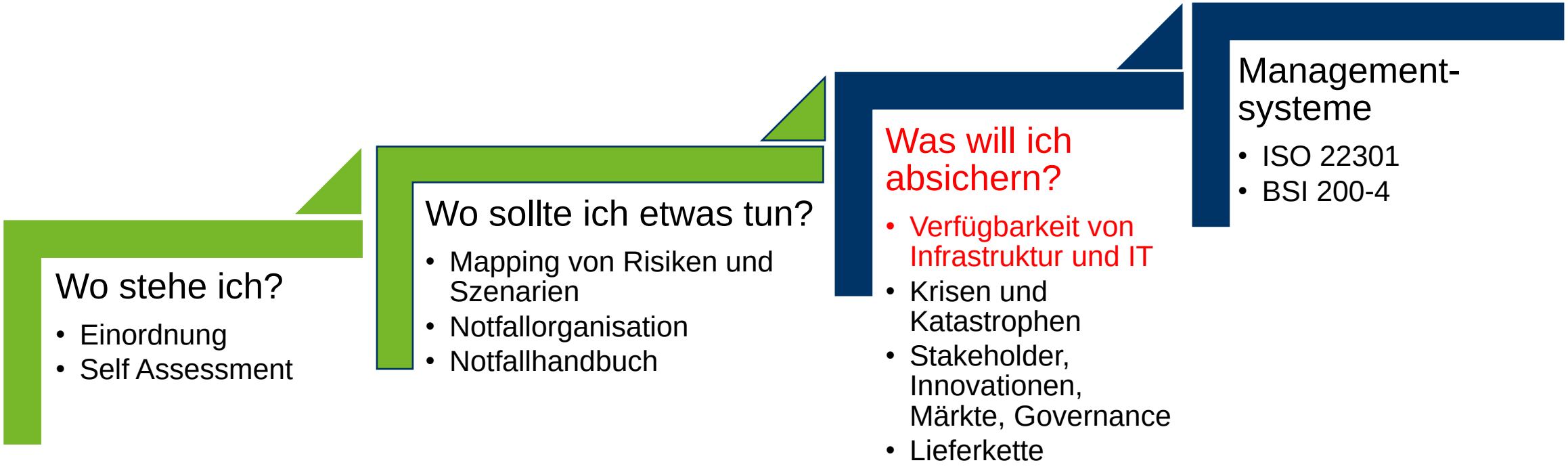
Überblick geben:
Was nützt Continuity Management?

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

Vortragsreihe



Agenda für heute

- **Einordnung**
  - Systematik
  - IT- und BCM-Organisation
- **Grundlagen: IT-Grundschutz nach BSI 200-2**
- **Szenario IT-Verfügbarkeit**
  - Eineinandergreifen der Komponenten
  - Erfassung von Infrastruktur/Systemen, Anwendungen und Prozessen
  - Beispiele
  - Nutzen
- **Bewertung und Ausblick**

Heute rauchen die Köpfe!

Agenda für heute

Haben Sie Erwartungen für heute?
Schreiben Sie es in den Chat !

Einordnung

IHK Südlicher Oberrhein

SDCON

Systematik

1. Self Assessment
2. Mapping Inventar und Prozesse
   Prüfung Konsistenz und Lücken
3. Risikobasiertes Resilienzmodell

Self Assessment

- **Auswahl der relevanten Maßnahmen/Themen**
  - Festlegen/Aktivieren der bewertungsrelevanten Maßnahmen/Themen
  - Filtern auf relevante Maßnahmen/Themen
  - Bewertung und Ableitung Handlungsbedarf

Systematik

1.
   - Self Assessment
2.
   - Mapping Inventar und Prozesse
   - Prüfung Konsistenz und Lücken
3.
   - Risikobasiertes Resilienzmodell

Mapping Inventar/Systeme, Prozesse und Anwendungen

- **Erfassung und Bewertung Inventar / Systemen, Prozessen und Anwendungen**
- **Maßnahmen des Assessments werden ergänzt um Bezugszahlen zu Inventaren, Anwendungen und Prozesse**
- **Konsistenzprüfung und Konsistenzlücken**
  - Sind zu allen relevanten Maßnahmen Prozess- und Inventarbezüge vorhanden?
  - Haben alle relevanten Inventare/Prozesse einen Bezug zu Maßnahmen?

Systematik

1. Self Assessment
2. Mapping Inventar und Prozesse
   Prüfung Konsistenz und Lücken
3. Risikobasiertes Resilienzmodell

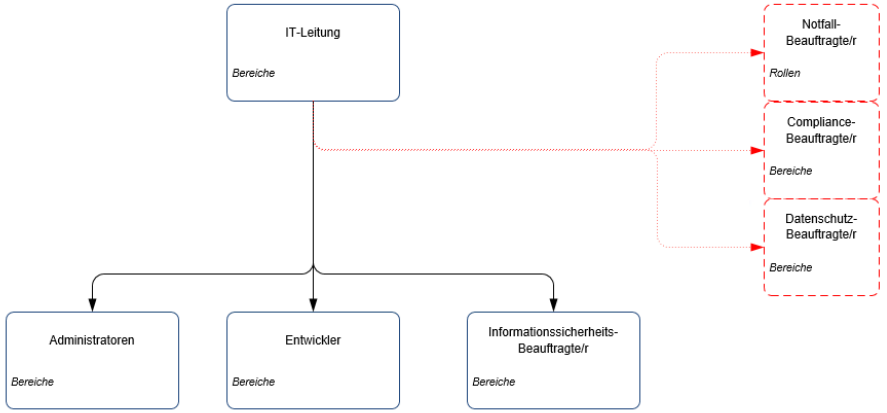
Risikobasierte Resilienz

- **Nutzen**
  - Bewertung von Risiken und Schadensauswirkungen
  - Vergleich mit Vorgabe zur Wiederherstellungszeit (SOLL)
- **Bei Verstoß gegen SOLL-Vorgabe:**
  - Bewertung der Möglichkeiten zur Erhöhung der Resilienz, Initiierung von Verbesserungsmaßnahmen
  - Übersicht in „BIA light“: Wo sind Bezüge und Verstöße?
  - Vergleich mit Wiederanlaufplan auf Konsistenz

Diese Systematik wird auf alle Szenarien angewendet

Rollen und Organigramm

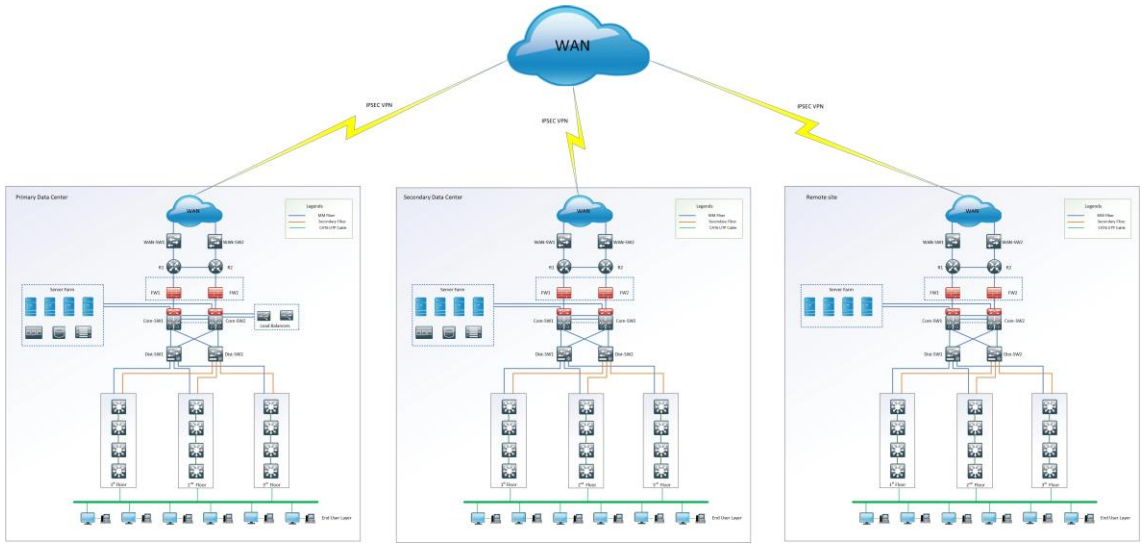
- **Berücksichtigung relevanter Rollen im Rahmen des Grundschutzes, z.B.**
  - Datenschutz-Beauftragte/r
  - Compliance-Beauftragte/r
  - Notfall-Beauftragte/r
  - Auditor/Revisor*in



Neue Rollenbezeichnung
Compliance-Beauftragte
Bauleitung
Benutzende
Bereichssicherheitsbeauftragte
Brandschutzbeauftragte
Datenschutzbeauftragte
Entwickelnde
ICS-Informationssicherheitsbeauftragte
Informationssicherheitsbeauftragte (ISB)
Mitarbeitende
Notfallbeauftragte
OT-Leitung
Planende
Testende

Netzwerktopologie

- **Bereichs- und Anlagen-Layout mit Darstellung von Redundanzen**
  - Anbindung der Standorte und des Rechenzentrums
  - Router und Aktivkomponenten
  - Firewall und DMZ
  - Server-Netzsegmente
  - Client-Netzsegmente
  - Ggf. weitere Segmente (z.B. Produktion



Quelle: Fiverr

Grundlagen

IHK Südlicher Oberrhein

SDCON

BSI-Standards

- BSI-Standard 200-1: Managementsysteme für Informationssicherheit
- BSI-Standard 200-2: IT-Grundschutz-Methodik
- BSI-Standard 200-3: Risikomanagement
- BSI-Standard 200-4: Business Continuity Management
- BSI-Standard 100-4: Notfallmanagement

Wer hat sich schon mit den BSI-Standards beschäftigt?

Grundlagen: IT-Grundschutz

Es geht NICHT um…

- detaillierte IT-technische Verfügbarkeit
- Diskussionen zur Verbesserung der Verfügbarkeit einzelner Anwendungen, Hardware und Technologien

Es geht um…

- einen systematischen Ansatz, um BCM auf die IT anzuwenden

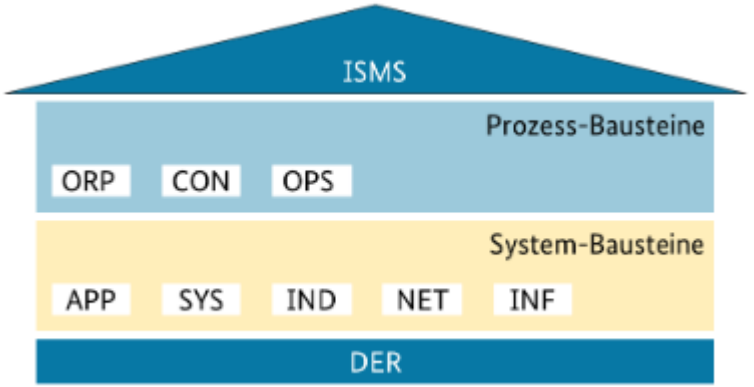
IT-Grundschutz-Kompendium

- **Grundlegende Veröffentlichung des IT-Grundschutzes**
  - IT-Grundschutz-Bausteine beleuchten relevante Sicherheitsaspekte
  - Orientierung an Gefährdungen und Sicherheitsanforderungen
  - Neben technischen Aspekten werden auch infrastrukturelle, organisatorische und personelle Themen betrachtet. Dies ermöglicht ein systematisches Vorgehen, um notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen.

Unterlagen zum BSI-Grundschutz finden Sie hier:
https://www.bsi.bund.de/dok/10027846

Das Schichtenmodell des IT-Grundschutzes

- **Systembausteine**
  - APP: Absicherung von Anwendungen und Diensten
  - SYS: Sicherheitsaspekte von IT-Systemen
  - NET: Sicherheitsaspekte von Netzwerk und Kommunikation
  - INF: baulich-technische Sicherheit, u.a. Gebäude und Rechenzentrum
  - IND: Sicherheit industrieller IT wie z.B. Maschinen, Sensoren, SPS
- **Prozessbausteine**
  - ISMS: Sicherheitsmanagement
  - ORP: organisatorische und personelle Sicherheitsaspekte
  - CON: Konzept und Vorgehensweise, u.a. Datenschutz und Krypto
  - OPS: Sicherheitsaspekte des operativen Betriebs
  - DER: Überprüfung der umgesetzten Sicherheitsmaßnahmen



Quelle: IT-Grundschutz-Kompendium, S. 25

Systembausteine

- **Auflistung der Systembausteine IND, INF, NET, APP**
  - Bewertung in Inventar und Anwendungen in Bezug auf Grundschutz-Einhaltung
  - Bewertung der BCM-Auswirkung
  - Anwendungs-System-Matrix bildet Abhängigkeiten zwischen Anwendungen und Systemen ab

APP-Baustein	Bezeichnung
APP.1.1	Office-Produkte
APP.1.2	Webbrowser
APP.1.4	Mobile Anwendungen
APP.2.1	Allgemeiner Verzeichnisdienst
APP.2.2	Active Directory Domain Services
APP.2.3	OpenLDAP
APP.3.1	Webanwendungen und Webservices
APP.3.2	Webserver
APP.3.3	Fileserver
APP.3.4	Samba
APP.3.6	DNS-Server
APP.4.2	SAP-ERP-System
APP.4.3	Relationale Datenbanken
APP.4.4	Kubernetes
APP.4.6	SAP ABAP-Programmierung
APP.5.2	Microsoft Exchange und Outlook
APP.5.3	Allgemeiner E-Mail-Client und -Server
APP.5.4	Unified Communications und Collaboration (UCC)
APP.6	Allgemeine Software
APP.7	Entwicklung von Individualsoftware

	Bezeichnung
	matisierungstechnik
	onente
	are Steuerung (SPS)
IND.2.7	Safety Instrumented Systems
IND.3.2	Fernwartung im industriellen Umfeld
INF.1	Allgemeines Gebäude
INF.2	Rechenzentrum sowie Serverraum
INF.5	Raum sowie Schrank für technische Infrastruktur
INF.6	Datenträgerarchiv
INF.7	Büroarbeitsplatz
INF.8	Häuslicher Arbeitsplatz
INF.9	Mobiler Arbeitsplatz
INF.10	Besprechungs-, Veranstaltungs- und Schulungsräume
INF.11	Allgemeines Fahrzeug
INF.12	Verkabelung
INF.13	Technisches Gebäudemanagement
INF.14	Gebäudeautomation
NET.1.1	Netzwerkarchitektur und -design
NET.1.2	Netzmanagement
NET.2.1	WLAN-Betrieb
NET.2.2	WLAN-Nutzung
NET.3.1	Router und Schwitches
NET.3.2	Firewall
NET.3.3	VPN
NET.3.4	Network Access Control
NET.4.1	TK-Anlagen
NET.4.2	VoIP
NET.4.3	Faxgeräte und Faxserver

Download:
https://service.sd-con.de/containerDocs/7987E74C

Prozessbausteine

- **Auflistung der Prozessbausteine**
  - Bewertung von allgemeinen IT-Prozessen in Bezug auf Grundschutz-Einhaltung
  - Bewertung der BCM-Auswirkung
- **Zuordnungen:**
  - Bereich IT, Bausteinname, Teilprozess
  - Kennzeichnung Spalte BSI-200-2

Unternehmens-bereich	Prozess/ Dokument	Teilprozess	BSI 200-2
IT	ORP	Organisation	X
IT	CON	Datenschutz	X
IT	CON	Datensicherungskonzept	X
IT	CON	Entwicklung von Webanwendungen	X
IT	CON	Informationsaustausch	X
IT	CON	Informationssicherheit auf Auslandsreisen	X
IT	CON	Kryptokonzept	X
IT	CON	Löschen und Vernichten	X
IT	CON	Software-Entwicklung	X
IT	DER	Audits und Revisionen	X
IT	DER	Behandlung von Sicherheitsvorfällen	X
IT	DER	Bereinigung weitreichender Sicherheitsvorfälle	X
IT	DER	Detektion von sicherheitsrelevanten Ereignissen	X
IT	DER	Notfallmanagement	X
IT	DER	Revisionen auf Basis des Leitfadens IS-Revision	X
IT	DER	Vorsorge für die IT-Forensik	X
IT	ISMS	Sicherheitsmanagement	X
IT	OPS	Allgemeiner IT-Betrieb	X
IT	OPS	Anbieten von Outsourcing	X
IT	OPS	Archivierung	X
IT	OPS	Cloud-Nutzung	X
IT	OPS	Fernwartung	X
IT	OPS	NTP-Zeitsynchronisation	X
IT	OPS	Nutzung von Outsourcing	X
IT	OPS	Ordnungsgemäße IT-Administration	X
IT	OPS	Patch- und Änderungsmanagement	X
IT	OPS	Protokollierung	X
IT	OPS	Schutz vor Schadprogrammen	X
IT	OPS	Software-Tests und Freigaben	X
IT	OPS	Systemmanagement	X
IT	OPS	Telearbeit	X
IT	ORP	Compliance Management / Anforderungsmanagement	X
IT	ORP	Identitäts- und Berechtigungsmanagement	X
IT	ORP	Personal	X
IT	ORP	Sensibilisierung und Schulung zur Informationssicherheit	X

Download:
https://service.sd-con.de/containerDocs/7987E74C

Tools und Hilfsmittel

Links:

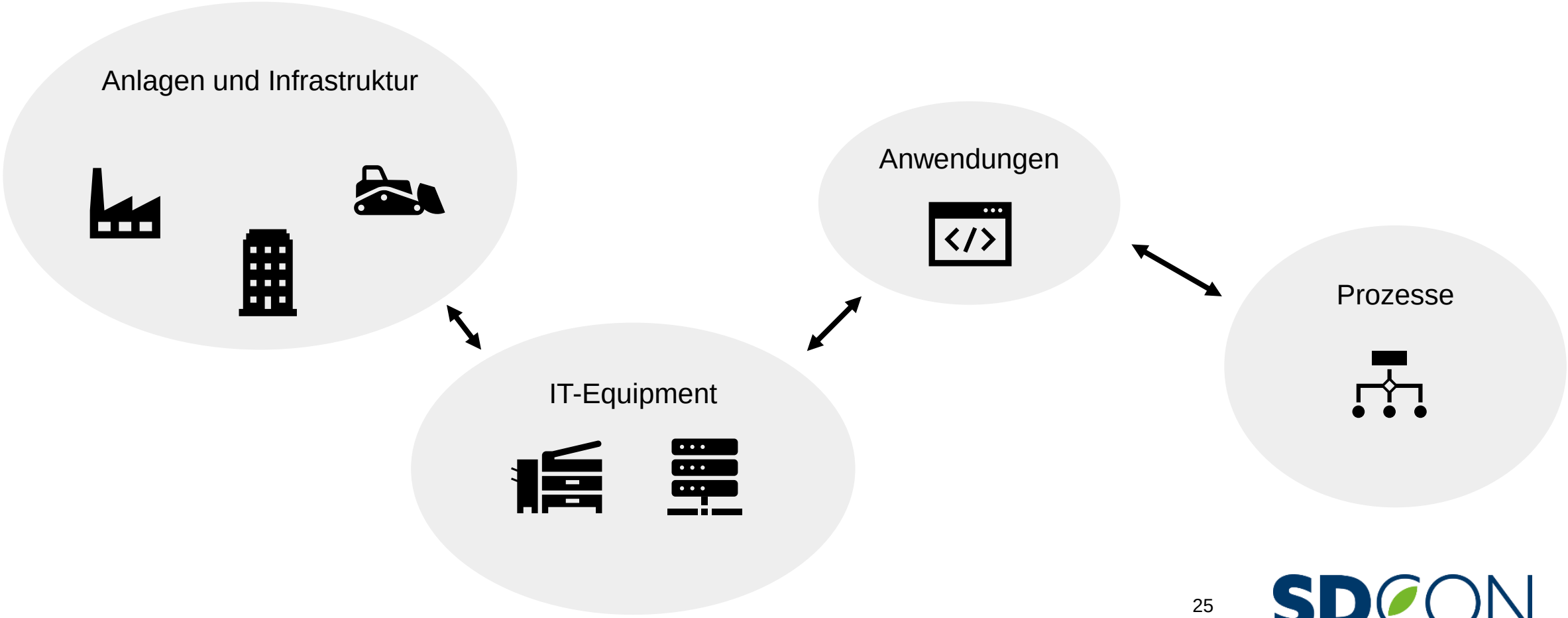
- **BSI 200—2 IT-Grundschutz-Methodik**
- **IT-Grundschutz-Kompendium**
- **Wege in die Basis-Absicherung (WiBA)**
- **Liste der System- und Anwendungs-Bausteine: https://service.sd-con.de/containerDocs/7987E74C**

Szenario IT-Verfügbarkeit

IHK Südlicher Oberrhein

SDCON

Ineinandergreifen der Komponenten



Inventarisierung ergänzt um Systembausteine

- **Übersicht der Infrastruktur:**
  - Filter auf relevante Unternehmensbereiche
  - Bezüge zu BCM-Maßnahmen prüfen
- **Ergänzung**
  - Bezug zu BSI 200-2
  - Bezug zu Baustein

Unternehmensbereich	Bezeichnung	Bezug zu BSI 200-2	Bausteine	Bezug zu BCM-Maßnahme
Lager	Abfalllager			Versorgungssicherheit gewährleisten
Produktion	Absaugeinrichtungen	X	IND	Betrieb aufrechterhalten
Produktion	Abwasser-behandlungsanlage	X	IND	IT-Grundschutz sicherstellen
Produktion	Abwasser-behandlungsanlage	X	IND	Gesetzesverstöße vermeiden
Produktion	Abwasser-behandlungsanlage	X	IND	Betrieb aufrechterhalten
Produktion	Anlagen mit IeD-Relevanz	X	IND	IT-Grundschutz sicherstellen
Produktion	Anlagen mit IeD-Relevanz	X	IND	Gesetzesverstöße vermeiden
Produktion	Anlagen mit Kühlschmierstoffen			Gesetzesverstöße vermeiden
Produktion	Anlagen mit Kühlschmierstoffen			Unfälle vermeiden/abwickeln
Produktion	Anlagen zur Beschichtung	X	IND	Betrieb aufrechterhalten
Produktion	Anlagen zur Lackierung	X	IND	IT-Grundschutz sicherstellen
Produktion	Anlagen zur Lackierung	X	IND	Betrieb aufrechterhalten
Produktion	Anlagen zur Schmelze	X	IND	IT-Grundschutz sicherstellen
Produktion	Anlagen zur Schmelze	X	IND	Betrieb aufrechterhalten
Infrastruktur/Gebäude	Auffangwannen			Unfälle vermeiden/abwickeln
Infrastruktur/Gebäude	Aufzüge (Personen- und Lastenaufzüge und Güterbeförderung)	X	IND	Betrieb aufrechterhalten
Lager	Automatisches Lager			Betrieb aufrechterhalten
Infrastruktur/Gebäude	Batterieladeanlagen			Infrastruktur erfassen, bewerten und

Übersicht der Anwendungen

- **Übersicht der Anwendungen**
  - Auflistung der Anwendungen, Zuordnung zu Typ
  - Bezug zu Systemtyp gem. Inventar
    Betriebssystem / Cloud
  - Bewertung der Software gem. BSI 200-2;
    Für nicht-vorhandene Checklisten kann eine Allgemeine Checkliste erstellt oder eine Checkliste der Softwarekategorie angepasst werden

Anwendungsbezeichnung	Anwendungstyp	Betriebssystem	Bezug zu BSI 200-2	Bausteine
Acronis Cloud Backup	System	Cloud		
CASQ-it	CAQ	MS Windows Server		
ConSense	IMS	MS Windows Server		
Cubeware	BI/BW	MS Windows Server		
Hintbox	Compliance	Cloud		
M-Files	DMS/ECM	MS Windows Server		
MS Active Directory	System	MS Windows Server	X	APP
MS Dynamics CRM	CRM	MS Windows Server		
MS Dynamics NAV	ERP	MS Windows Server	X	APP (SAP)
MS Exchange	Groupware	MS Windows Server	X	APP
MS Hyper-V	System	MS Windows Server		
MS Office 365	Office	MS Windows Server	X	APP
MS Project	PM / Project Man.	MS Windows Server		
MS Sharepoint	DMS/ECM	MS Windows Server		
MS SQL Server	DBMS	MS Windows Server	X	APP
MS Teams	Groupware	MS Windows Server	X	APP
MS Visio	Office	MS Windows Server		
Nagios	System	Linux		
Panda Adaptive Defense	Security	Cloud		
Signavio	BPM	MS Windows Server		
Typo3	DMS/ECM	Linux	X	APP

Anwendungs-System-Matrix

- **Abbildung einer Anwendungs-System-Matrix zur Abbildung von Abhängigkeiten**

Anwendungsbezeichnung	Anwendungstyp	Betriebssystem	Webserver Cloud	App-Server 1	App-Server 2	App-Server 3	Virtualisierung 1	Virtualisierung 2	Virtualisierung 3	Terminalserver 1	Terminalserver 2
Acronis Cloud Backup	System	Cloud									
CASQ-it	CAQ	MS Windows Server				x					
ConSense	IMS	MS Windows Server						x			
Cubeware	BI/BW	MS Windows Server						x			
Hintbox	Compliance	Cloud									
M-Files	DMS/ECM	MS Windows Server						x			
MS Active Directory	System	MS Windows Server					x				
MS Dynamics CRM	CRM	MS Windows Server							x		
MS Dynamics NAV	ERP	MS Windows Server							x		
MS Exchange	Groupware	MS Windows Server							x		
MS Hyper-V	System	MS Windows Server					x	x	x		
MS Office 365	Office	MS Windows Server								x	x
MS Project	PM / Project Man.	MS Windows Server								x	x
MS Sharepoint	DMS/ECM	MS Windows Server		x							
MS SQL Server	DBMS	MS Windows Server		x		x			x		
MS Teams	Groupware	MS Windows Server								x	x
MS Visio	Office	MS Windows Server								x	x
Nagios	System	Linux			x						
Panda Adaptive Defense	Security	Cloud									
Signavio	BPM	MS Windows Server						x			
Typo3	DMS/ECM	Linux	x								

Prozesse ergänzt um Prozessbausteine

- **Übersicht der Prozesse**
  - Filter auf relevante Unternehmensbereiche
- **Ergänzung**
  - Bezug zu BSI 200-2
  - Bezug zu Baustein

Unternehmens-bereich	Prozess/ Dokument	Teilprozess	Bezug zu BSI 200	Bausteine
HR	Ressourcen Allgemein	Personal	X	ORP
IMS	IT-Security	Datenschutz	X	CON
IT	IT-Apps	Anbieten von Outsourcing	X	OPS
IT	IT-Apps	Entwicklung von Webanwendungen	X	CON
IT	IT-Apps	Nutzung von Outsourcing	X	OPS
IT	IT-Apps	Software-Entwicklung	X	CON
IT	IT-Apps	Software-Tests und Freigaben	X	OPS
IT	IT-Infrastruktur	Allgemeiner IT-Betrieb	X	OPS
IT	IT-Infrastruktur	Fernwartung	X	OPS
IT	IT-Infrastruktur	Löschen und Vernichten	X	CON
IT	IT-Infrastruktur	Ordnungsgemäße IT-Administration	X	OPS
IT	IT-Infrastruktur	Patch- und Änderungsmanagement	X	OPS
IT	IT-Infrastruktur	Systemmanagement	X	OPS
IT	IT-Orga	Organisation	X	ORP
IT	IT-Security	Behandlung von Sicherheitsvorfällen	X	DER
IT	IT-Security	Bereinigung weitreichender Sicherheitsvorfälle	X	DER
IT	IT-Security	Detektion von sicherheitsrelevanten Ereignissen	X	DER
IT	IT-Security	Datensicherungskonzept	X	CON
IT	IT-Security	Identitäts- und Berechtigungsmanagement	X	ORP
IT	IT-Security	Informationsaustausch	X	CON
IT	IT-Security	Informationssicherheit auf Auslandsreisen	X	CON
IT	IT-Security	Kryptokonzept	X	CON
IT	IT-Security	Notfallmanagement	X	DER
IT	IT-Security	Revisionen auf Basis des Leitfadens IS-Revision	X	DER
IT	IT-Security	Schutz vor Schadprogrammen	X	OPS
IT	IT-Security	Sensibilisierung und Schulung zur Informationssicherheit	X	ORP
IT	IT-Security	Telearbeit	X	OPS
IT	IT-Security	Vorsorge für die IT-Forensik	X	DER
IT	IT-Infrastruktur	Archivierung	X	OPS
IT	IT-Orga	Audits und Revisionen	X	DER
IT	IT-Apps	Cloud-Nutzung	X	OPS
IT	IT-Orga	Compliance Management / Anforderungsmanagement	X	ORP
IT	IT-Infrastruktur	NTP-Zeitsynchronisation	X	OPS
IT	IT-Infrastruktur	Protokollierung	X	OPS
IT	IT-Security	Sicherheitsmanagement	X	ISMS

Beispiele

IHK Südlicher Oberrhein

SDCON

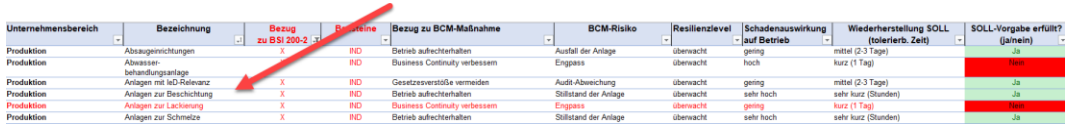
Rechenzentraum / Serverraum

- **Prüfung in Infrastruktur/Inventarliste**
  - Bezug zu IT-Grundschutz
  - Bezug zu Maßnahmen und Risiko
- **Bewertung Baustein INF.2**
  - Filter auf Vorgabentyp (Basis, Standard, Hoch)
  - Bewertung der Entbehrlichkeit bzw. BCM-Auswirkung
  - Filter auf nicht-entbehrliche Anforderungen
  - Übertragung der Bewertung in BCM-Inventarliste
- **Bewertung der BCM-Auswirkung**

Unternehmens-bereich	OU	Bezug zu BSI 200-2	Bezeichnung	Bezug zu BCM-Maßnahme	BCM-Risiko	SOLL-Vorgabe erfüllt? (ja/nein)	Resilienzwirkung	Ergriffene Aktion
IT	INF	X	Serverraum	IT-Grundschutz sicherstellen	Nicht-Einhaltung der Anforderungen	Nein	Normvorgabe beachten	Feststellungen aus INF.2 umsetzen
IT	INF	X	Serverraum	Unbefugtes Eindringen vermeiden	Unbefugter Zugriff	Nein	Fehlerfreundlichkeit verbessern	Feststellungen aus INF.2 umsetzen

Automatische Lackieranlage

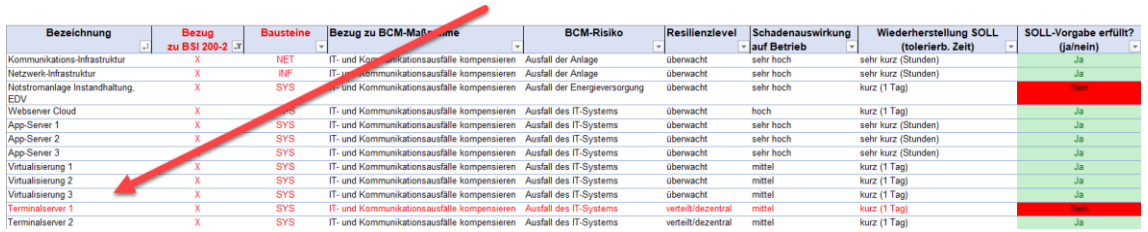
- **Prüfung in Infrastruktur/Inventarliste**
  - „Eine Maschine ist eine techn. Vorrichtung, die automatisiert Aufgaben durchführt. Ein typisches Beispiel dafür ist eine Werkzeugmaschine, die Werkstücke auf eine vorgegebene Art bearbeitet. Dabei wird sie von einem IT-System gesteuert, …“
  - Bezug zu IT-Grundschutz
  - Bezug zu Maßnahmen und Risiko
- **Bewertung Baustein IND.2.4**
  - Bewertung der Entbehrlichkeit bzw. BCM-Auswirkung
  - Filter auf nicht-entbehrliche Anforderungen
  - Übertragung der Bewertung in BCM-Inventarliste
- **Bewertung der BCM-Auswirkung**



Unternehmensbereich	Bezeichnung	Bezug zu BSI 200-2	Bausteine	Bezug zu BCM-Maßnahme	BCM-Risiko	Resilienzlevel	Schadenauswirkung auf Betrieb	Wiederherstellung SOLL (tolerierb. Zeit)	SOLL-Vorgabe erfüllt? (ja/nein)
Produktion	Absaugeinrichtungen	X	IND	Betrieb aufrechterhalten	Ausfall der Anlage	überwacht	gering	mittel (2-3 Tage)	Ja
Produktion	Abwasser-behandlungsanlage		IND	Business Continuity verbessern	Engpass	überwacht	hoch	kurz (1 Tag)	Nein
Produktion	Anlagen mit IdD-Relevanz	X	IND	Gesetzesverstöße vermeiden	Audit-Abweichung	überwacht	gering	mittel (2-3 Tage)	Ja
Produktion	Anlagen zur Beschichtung	X	IND	Betrieb aufrechterhalten	Stillstand der Anlage	überwacht	sehr hoch	sehr kurz (Stunden)	Ja
Produktion	Anlagen zur Lackierung	X	IND	Business Continuity verbessern	Engpass	überwacht	gering	kurz (1 Tag)	Nein
Produktion	Anlagen zur Schmelze	X	IND	Betrieb aufrechterhalten	Stillstand der Anlage	überwacht	sehr hoch	sehr kurz (Stunden)	Ja

Windows Server / Terminalserver

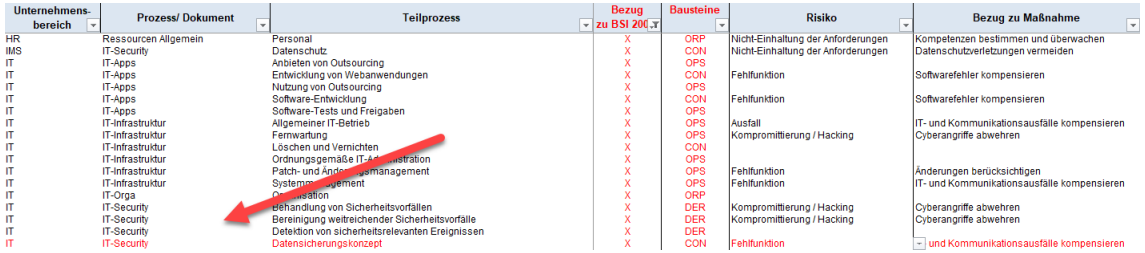
- **Prüfung in Infrastruktur/Inventarliste**
  - Bezug zu IT-Grundschutz
  - Bezug zu Maßnahmen und Risiko
- **Bewertung Baustein SYS.1.9**
  - Beachten: Einige BCM-relevante Aspekte sind in den Absicherungslevels Standard / Hoch enthalten
  - Bewertung der Entbehrlichkeit bzw. BCM-Auswirkung. Unter Härtung/Hochverfügbarkeit sind BCM-relevante Aspekte genannt
  - Filter auf nicht-entbehrliche Anforderungen
  - Übertragung der Bewertung in BCM-Inventarliste
- **Bewertung der BCM-Auswirkung**



Bezeichnung	Bezug zu BSI 200-2	Bausteine	Bezug zu BCM-Maßnahme	BCM-Risiko	Resilienzlevel	Schadenauswirkung auf Betrieb	Wiederherstellung SOLL (tolerierb. Zeit)	SOLL-Vorgabe erfüllt? (ja/nein)
Kommunikations-Infrastruktur	X	NET	IT- und Kommunikationsausfälle kompensieren	Ausfall der Anlage	überwacht	sehr hoch	sehr kurz (Stunden)	Ja
Netzwerk-Infrastruktur	X	INF	IT- und Kommunikationsausfälle kompensieren	Ausfall der Anlage	überwacht	sehr hoch	sehr kurz (Stunden)	Ja
Notstromanlage Instandhaltung, EDV	X	SYS	IT- und Kommunikationsausfälle kompensieren	Ausfall der Energieversorgung	überwacht	sehr hoch	kurz (1 Tag)	Nein
Webserver Cloud	X	SYS	IT- und Kommunikationsausfälle kompensieren	Ausfall des IT-Systems	überwacht	hoch	kurz (1 Tag)	Ja
App-Server 1	X	SYS	IT- und Kommunikationsausfälle kompensieren	Ausfall des IT-Systems	überwacht	sehr hoch	sehr kurz (Stunden)	Ja
App-Server 2	X	SYS	IT- und Kommunikationsausfälle kompensieren	Ausfall des IT-Systems	überwacht	sehr hoch	sehr kurz (Stunden)	Ja
App-Server 3	X	SYS	IT- und Kommunikationsausfälle kompensieren	Ausfall des IT-Systems	überwacht	sehr hoch	sehr kurz (Stunden)	Ja
Virtualisierung 1	X	SYS	IT- und Kommunikationsausfälle kompensieren	Ausfall des IT-Systems	überwacht	mittel	kurz (1 Tag)	Ja
Virtualisierung 2	X	SYS	IT- und Kommunikationsausfälle kompensieren	Ausfall des IT-Systems	überwacht	mittel	kurz (1 Tag)	Ja
Virtualisierung 3	X	SYS	IT- und Kommunikationsausfälle kompensieren	Ausfall des IT-Systems	überwacht	mittel	kurz (1 Tag)	Ja
Terminalserver 1	X	SYS	IT- und Kommunikationsausfälle kompensieren	Ausfall des IT-Systems	verteilt/dezentral	mittel	kurz (1 Tag)	Nein
Terminalserver 2	X	SYS	IT- und Kommunikationsausfälle kompensieren	Ausfall des IT-Systems	verteilt/dezentral	mittel	kurz (1 Tag)	Ja

Datensicherungskonzept

- **Prüfung in Prozessen**
  - Bezug zu IT-Grundschutz
  - Bezug zu Maßnahmen und Risiko
- **Bewertung Baustein CON.3**
  - Beachten: Einige BCM-relevante Aspekte sind in den Absicherungslevels Standard / Hoch enthalten
  - Bewertung der Entbehrlichkeit bzw. BCM-Auswirkung. Unter Härtung/Hochverfügbarkeit sind BCM-relevante Aspekte genannt
  - Filter auf nicht-entbehrliche Anforderungen
  - Übertragung der Bewertung in BCM-Inventarliste
- **Bewertung der BCM-Auswirkung**



Unternehmens-bereich	Prozess/ Dokument	Teilprozess	Bezug zu BSI 200	Bausteine	Risiko	Bezug zu Maßnahme
HR	Ressourcen Allgemein	Personal	X	ORP	Nicht-Einhaltung der Anforderungen	Kompetenzen bestimmen und überwachen
IMS	IT-Security	Datenschutz	X	CON	Nicht-Einhaltung der Anforderungen	Datenschutzverletzungen vermeiden
IT	IT-Apps	Anbieten von Outsourcing	X	OPS		
IT	IT-Apps	Entwicklung von Webanwendungen	X	CON	Fehlfunktion	Softwarefehler kompensieren
IT	IT-Apps	Nutzung von Outsourcing	X	OPS		
IT	IT-Apps	Software-Entwicklung	X	CON	Fehlfunktion	Softwarefehler kompensieren
IT	IT-Apps	Software-Tests und Freigaben	X	OPS		
IT	IT-Infrastruktur	Allgemeiner IT-Betrieb	X	OPS	Ausfall	IT- und Kommunikationsausfälle kompensieren
IT	IT-Infrastruktur	Fernwartung	X	OPS	Kompromittierung / Hacking	Cyberangriffe abwehren
IT	IT-Infrastruktur	Löschen und Vernichten	X	CON		
IT	IT-Infrastruktur	Ordnungsgemäße IT-Administration	X	OPS		
IT	IT-Infrastruktur	Patch- und Änderungsmanagement	X	OPS	Fehlfunktion	Änderungen berücksichtigen
IT	IT-Infrastruktur	Systemmanagement	X	OPS	Fehlfunktion	IT- und Kommunikationsausfälle kompensieren
IT	IT-Orga	Organisation	X	ORP		
IT	IT-Security	Behandlung von Sicherheitsvorfällen	X	DER	Kompromittierung / Hacking	Cyberangriffe abwehren
IT	IT-Security	Bereinigung weitreichender Sicherheitsvorfälle	X	DER	Kompromittierung / Hacking	Cyberangriffe abwehren
IT	IT-Security	Detektion von sicherheitsrelevanten Ereignissen	X	DER		
IT	IT-Security	Datensicherungskonzept	X	CON	Fehlfunktion	und Kommunikationsausfälle kompensieren

Wichtige Tools und Hilfsmittel

Links:

- **Excel-Listen der Bewertungs-Tools: https://service.sd-con.de/containerDocs/A97C037C**
- **Wiederanlaufplan: https://service.sd-con.de/containerDocs/3539D45A**

Nutzen

IHK Südlicher Oberrhein

SDCON

Zusammenführung

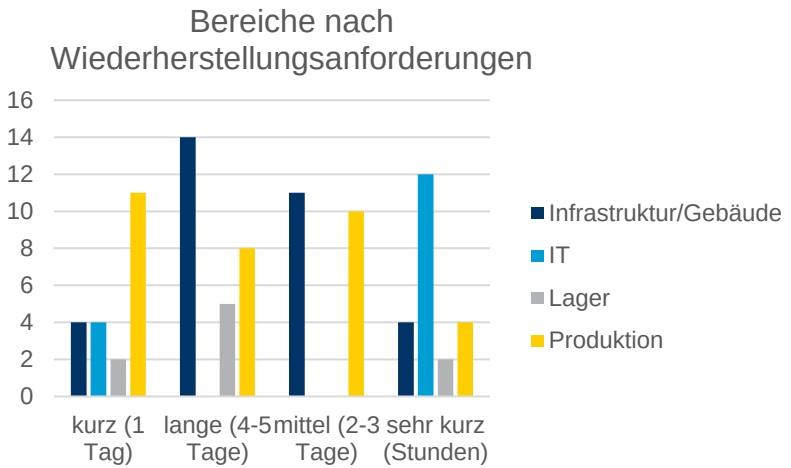
- **Anzahl der Maßnahmenbezüge und Verstöße werden in der „BIA light“ zusammengeführt**

BCM-Assessment und BIA light

Maßnahme	Relevanz zur Bewertung	Wichtigkeit der Erfüllung	Eigene Fähigkeit	Handlungs-bedarf	Anzahl Inventare	Verstöße	Anzahl Anwendungen	Verstöße	Anzahl Prozesse	Verstöße
Beauftragte/n einsetzen				0					0	
Bedienfehler kompensieren	X			0					0	
Betrieb aufrechterhalten	X	9	7	2	21	4			0	
Betrugsdelikte vermeiden/abwickeln		3	3	0					0	
Bewusstsein fördern				0					0	
Brände vermeiden, notfalls überstehen	X	9		9	1				0	
Business Continuity verbessern	X			0	6	2			1	
Business Impact Analyse durchführen				0					0	
Compliance Management umsetzen				0					0	
Compliance-Anforderungen erfassen		5		5					0	
Cyberangriffe abwehren	X	7	8	-1	1		1		3	
Datenschutzverletzungen vermeiden	X	9	9	0					1	
Dokumentierte Information und Nachweise führen				0			4		0	
Elementarschäden kompensieren	X			0					0	
Erste Hilfe leisten		9	9	0					0	
Forderungsausfälle absichern und kompensieren				0					0	
Gesetzesverstöße vermeiden	X			0	5	1			0	
Hinweise und Beschwerden erfassen und bewerten	X			0			1		0	
Informationssicherheit umsetzen	X			0					0	
Infrastruktur erfassen, bewerten und aufrechterhalten	X			0	15	1			2	
Instandhaltung sicherstellen	X			0	2				0	
IT- und Kommunikationsausfälle kompensieren	X	9	9	0	15	3	7	1	3	1
IT-Grundschutz sicherstellen	X	9	3	6					0	
Kommunikation regeln				0			2	1	1	

Auswertung

- **Einstufung der Wiederherstellungs-anforderungen**
  - Assets nach Zeiträumen
  - Bereiche nach Zeiträumen
- **Prüfung gegen Wiederanlaufplan**



		Anlaufphasen 1	2	3	5	6
Abteilungen						
Vertrieb						x
Einkauf						x
Produktion						x
Lager						x
QS						x
IT						
Anwendungen						
	CRM-System					x
	CAQ-System					x
	ERP-System					x
	Archivsystem				x	
	Datenbankserver 1				x	
	Mailserver			x		
	Zutrittskontrolle			x		
	Active Directory			x		
Systeme						
	Server 7					x
	Server 6					x
	Server 5					x
	Server 4				x	
	Server 3				x	
	Server 2			x		
	Server 1			x		
	ITK-Anlage		x			
	Backup-System		x			
	Firewall		x			
	Router und Switches		x			
Infrastruktur						
	USV	x				
	Stromversorgung	x				

Bewertung und Ausblick

Diskussionspunkte

- **Excel-Handling als zusätzliche Session interesssant?**
- **Weitere Excel-Szenarien**
  - Prozesse könnten mit Anwendungen gemapped werden
  - Reihenfolge des Wiederanlaufs mit den dazugehörigen Systemen und Anwendungen könnte in einer Pivottabelle analysiert werden
- **Grenzen von Excel**
  - Die Handhabung und Abbildung in Excel-Tabellen kommt an Grenzen und geht weit über den „versierten Anwender“ hinaus
  - Die Abbildung von BCM-Maßnahmen für unterschiedlichste Szenarien ist mir Excel nur sehr grob handhabbar
  - Bei strategischer Nutzung ist der Einsatz von ergänzender Software notwendig

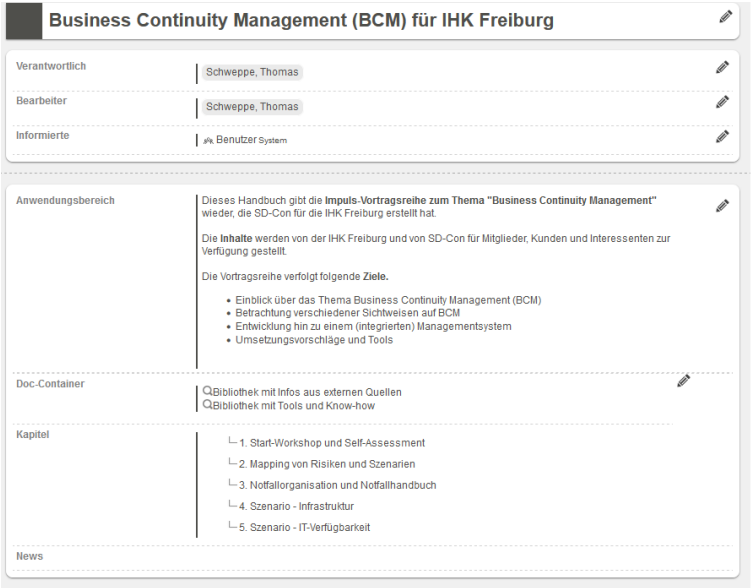
Ausblick

IHK Südlicher Oberrhein

SDCON

Ausblick

- **Weitere Szenarien für**
  - Governance: BCM und „gute Unternehmensführung“
  - Krisen und Katastrophen
  - Stakeholder, Innovationen, Märkte, Governance
  - Lieferkette
- **Systematisierung und Integration über ein System (z.B. ISO 22301, ISO 31000, GPG Good Practice Guidelines)**
- **Integrierte Abbildung Maßnahmen, Prozessen, Inventaren, Compliance über das SD-Serviceportal**



Und was jetzt?

Fragen bitte an:

Thomas Schweppe
t.schweppe@sd-con.de