Business Continuity Management für den Mittelstand

Scio GmbH für it-sa 2022

Frank Büttner, Markus Wolff

„Wir haben doch eine Firewall und unsere IT macht doch Backups!“

…aber die Realität sieht anders aus

Aerzener Maschinenfabrik

Cyberkriminelle verschlüsselten die Unternehmensdaten.

Das Unternehmen stand für 8 Wochen still mit 1100 Mitarbeitern in Kurzarbeit.

Es wurde entschieden, kein Lösegeld zu bezahlen, sondern das IT-Netzwerk vollständig neu aufzubauen.

Allein die Umsatzeinbußen betrugen etwa 30 Millionen Euro.

Betriebsausstatter Berger

Lieferkettenangriff über ein Software-Update von Kaseya; weltweit waren mehr als 1500 Unternehmen vom Angriff betroffen.

Erkennung des Angriffs durch IT-Frühwarnsystem bei Berger; deshalb nur geringe Ausbreitung.

Kein Zugriff auf Daten und sonstige Systeme führte zu einem Betriebsstillstand für 4 Tage.

Keine Lösegeldzahlung, da alle verschlüsselten Daten aus funktionierenden Backups wiederhergestellt werden konnten.

rational Einbauküchen

Erhebliche Beschädigung der Server mit irreparablem Datenverlust infolge eines Stromausfalls.

Produktionsstillstand, da Systeme für Produktion & Planung, sowie für weitere kritische Geschäftsprozesse nicht zur Verfügung stehen.

Was ist BCM?

BCM (Business Continuity Management) befasst sich mit der **Vorsorge gegen Ausfälle** des Geschäftsbetriebs und der **Vorbereitung der Geschäftsfortführung** im Schadensfall.

Mithilfe des BCM soll sichergestellt werden, dass sich Schadensereignisse nicht existenzbedrohend auf das Unternehmen auswirken.

Dies soll dadurch erreicht werden, dass der Geschäftsbetrieb bei Katastrophen möglichst nicht unterbrochen wird bzw. bei Ausfällen innerhalb angemessener Zeit auf einem Mindestniveau wieder fortgeführt werden kann.

Definition nach BSI 200-4

Gängige Standards im BCM im deutschsprachigen Raum

ISO 22301:2019 - Sicherheit und Resilienz – Business Continuity Management System - Anforderungen

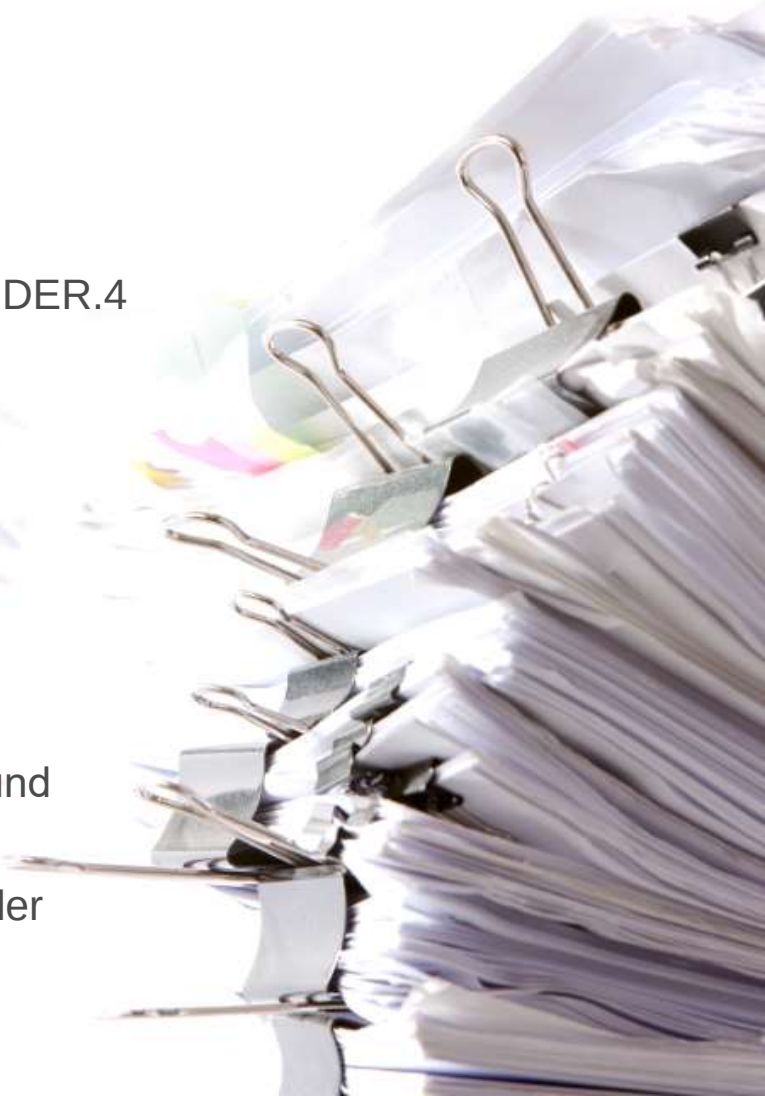
BSI-Standard 200-4 - Business Continuity Management

BSI-Standard 200-2 – IT-Grundschutz-Methodik: IT-Grundschutz-Kompendium Baustein DER.4 Notfallmanagement

KRITIS-Unternehmen aus 9 Sektoren: Energie, Gesundheit, Informationstechnik und Kommunikation, Transport und Verkehr, Medien und Kultur, Wasser, Finanz- und Versicherungswesen, Ernährung, Staat und Verwaltung.

BSI-Gesetz (BSIG) §8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen:

„Betreiber Kritischer Infrastrukturen sind verpflichtet […] angemessene organisatorische und technische Vorkehrungen zur Vermeidung von **Störungen der Verfügbarkeit**, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind.“



Wie „viel“ BCM benötige ich?

One size doesn‘t fit all

Kleinstbetriebe, Einfache Handwerksbetriebe	Kl. Agenturen, Kanzleien	Industrie-unternehmen	Online-Business Unternehmen	„KRITIS“ Unternehmen (z.B. Kliniken)

Sehr niedrig — **„IT-Abhängigkeit“** — Sehr hoch

„Minimalanspruch“:

- Business Impact Analysen
- „Professionelles“ BCM

- Priorität & Reihenfolge der Systeme festlegen
- Wiederherstellungspläne für die relevanten IT-Systeme erstellen

- Regelmäßig Backups der kritischen Daten nach der Fragestellung: Wie viel Daten darf ich maximal verlieren?
- Backup-Rücksicherung mind. 1x pro Jahr prüfen (→ Wiedereinspielen!)
- „Notfallhandbuch“ mit allen wichtigen Kontakten und Informationen (bspw. Systemadministrator, Versicherung)
- Bei Malware (bspw. Krypto-Trojaner): Prüfen, ob Backups kontaminiert sind, bevor wie wiedereingespielt werden!
- Hohe Abhängigkeit von Dienstleistern: Prüfen, ob dort ein angemessenes BCM / Notfallmanagement existiert

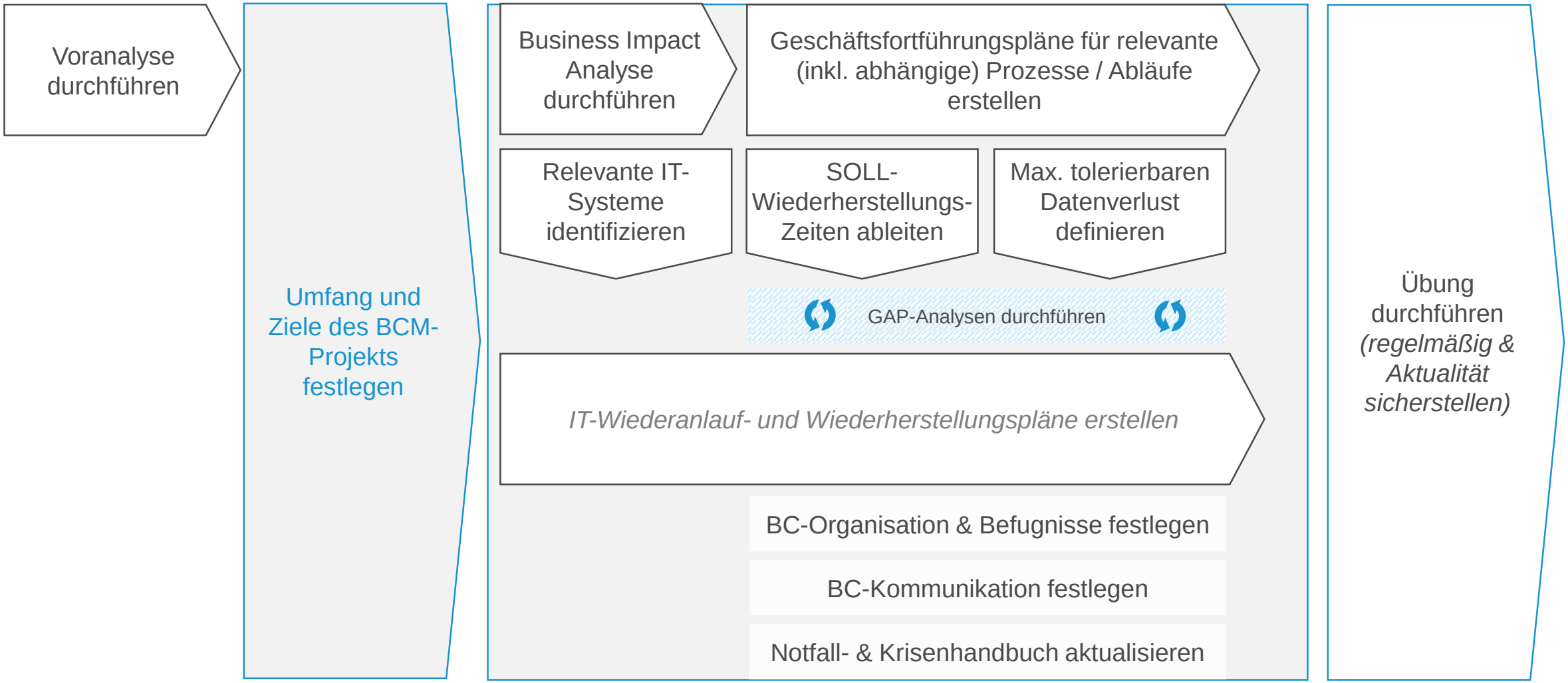
Wie gehe ich das Thema BCM an?

Was brauche ich?

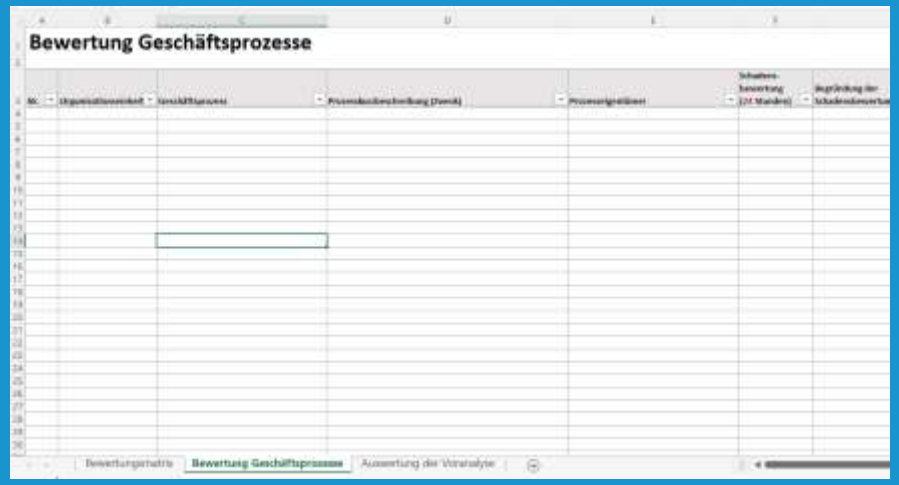
Was muss ich tun?

Wie gehe ich am besten vor?

Inhalte und Aufbau eines „BCM-Projekts“



Die Voranalyse: Aufwandssteuerung & schnelle Ergebnisse im BCM-Projekt.



Excel Vorlage zum Download:

https://www.scio.eu/bcm-voranalyse/

- **Einfach bleiben**; Ist der Prozess aus BCM-Sicht kritisch?
- **Kompakte Termine** mit den Prozessverantwortlichen! (Keine Workshop-Marathons!)
- **Schadenskategorien** für alle Prozesse **begründen lassen**!

BCM-Projekt aufsetzen:
Mindest-Ergebnisse des BCM-Projekts

Notfallhandbuch (reduzierte Version: Alarmierung, Sofortmaßnahmen, Kontaktlisten, Entscheidungsbefugnisse im K-Fall)

Leitlinie BCM (kompakte Version: Rahmen geben, „Warum mache ich BCM“ & Begrifflichkeiten)

Kommunikationsplan (Wann ist wer wie und durch wen zu informieren)

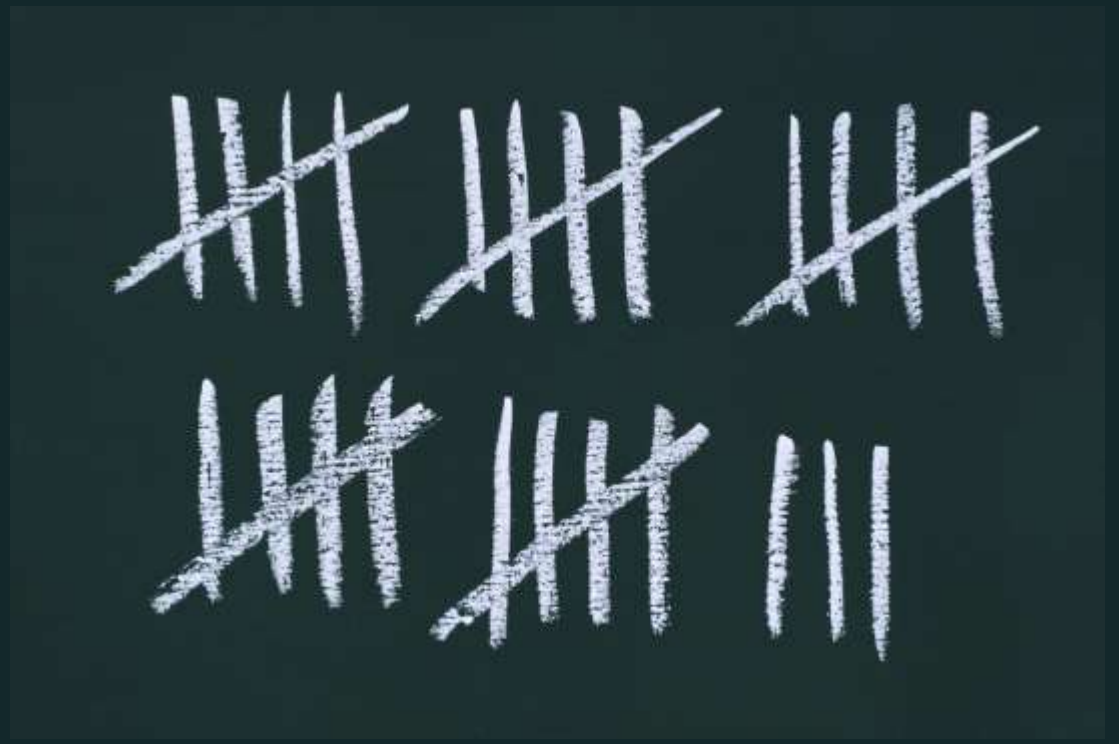
Geschäftsfortführungsplan (Notbesetzung, Besondere Befugnisse, (Wieder-) Anlauf Notbetrieb, Wie erfolgt der Notbetrieb, Rückführung in den Normalbetrieb, …)

Wiederherstellungs- und Wiederanlaufpläne (IT-Abhängigkeiten & Voraussetzungen, detaillierte „how-to“ Checkliste, Zeiten, Verantwortlichkeiten, Freigabe für den Notbetrieb, Rückführung in den Normalbetrieb)

Denken Sie bitte daran, die Pläne auch auszudrucken, so dass diese auch im Falle eines Ausfalls der IT-Systeme zur Verfügung

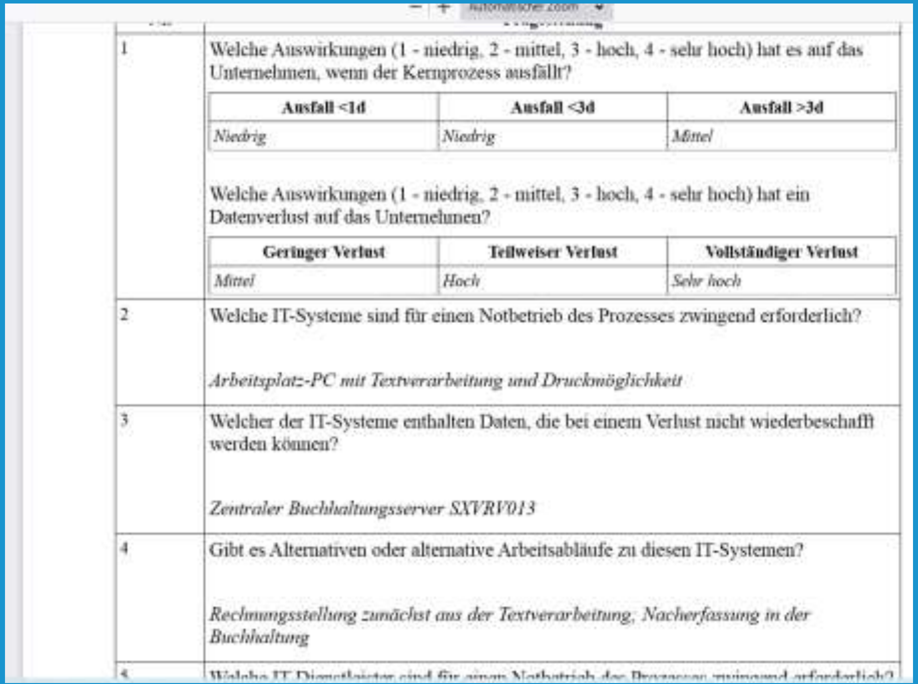
„Wir sind am wichtigsten!“

„Wir können auf nichts verzichten!“



Die Business Impact Analyse (BIA)

„Einfache“ BIA im Word-Format (→ überschaubare Anzahl an Prozessen & IT-Systemen kaum Abhängigkeiten)



1 Welche Auswirkungen (1 - niedrig, 2 - mittel, 3 - hoch, 4 - sehr hoch) hat es auf das Unternehmen, wenn der Kernprozess ausfällt?

Ausfall <1d	Ausfall <3d	Ausfall >3d
Niedrig	*Niedrig*	*Mittel*

Welche Auswirkungen (1 - niedrig, 2 - mittel, 3 - hoch, 4 - sehr hoch) hat ein Datenverlust auf das Unternehmen?

Geringer Verlust	Teilweiser Verlust	Vollständiger Verlust
Mittel	*Hoch*	*Sehr hoch*

2 Welche IT-Systeme sind für einen Notbetrieb des Prozesses zwingend erforderlich?

Arbeitsplatz-PC mit Textverarbeitung und Druckmöglichkeit

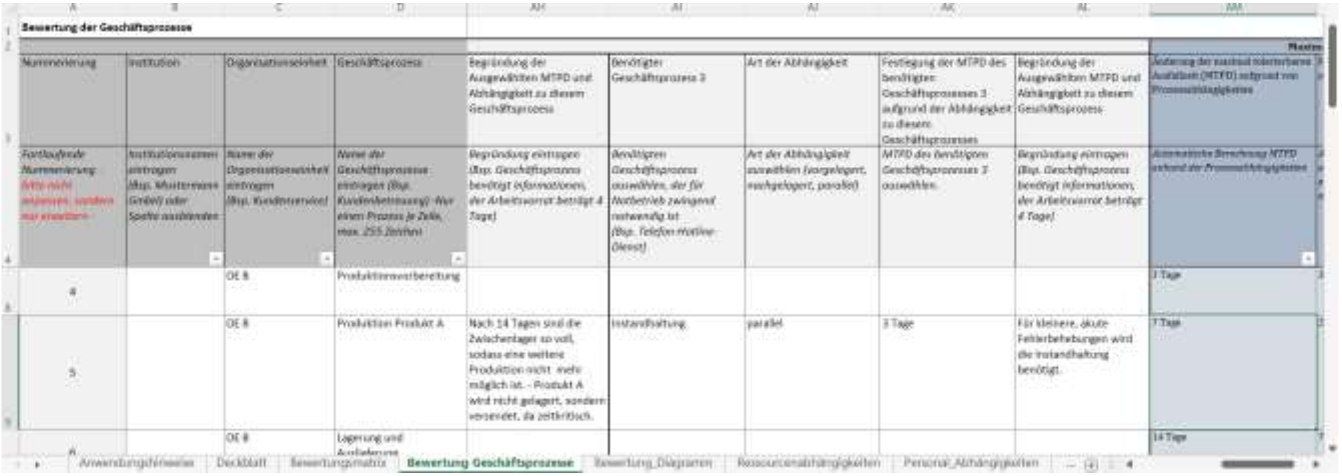
3 Welcher der IT-Systeme enthalten Daten, die bei einem Verlust nicht wiederbeschafft werden können?

Zentraler Buchhaltungsserver SXVRV013

4 Gibt es Alternativen oder alternative Arbeitsabläufe zu diesen IT-Systemen?

Rechnungsstellung zunächst aus der Textverarbeitung, Nacherfassung in der Buchhaltung

BIA im Excel-Format (höhere Komplexität)



Quelle: https://www.bsi.bund.de

Geschäftsfortführungspläne: Gängige BC-Strategien für IT-Ausfall

- **Nicht IT-bezogene Ausweichverfahren:** Workarounds durch Papierformulare, Kommunikation per Fax/Telefon. Sollten stets nur als temporäre Lösung genutzt werden.
- **Zeitkritische Daten physikalisch vorhalten:** Vorhalten von z.B. Passwörtern, Kontaktlisten etc. in Papierform an einem sicheren Ort (z.B. Tresor).
- **Vorhalten von Ersatzhardware:** Im Falle von besonders hoher Zeitkritikalität sollten Ersatzhardwarekomponenten in ausreichender Anzahl, wie z.B. Server, Notebooks Drucker, Festplatten etc. vorgehalten werden.
- **Nutzung externer IT-Services:** Als Alternative zu einem zweiten Rechenzentrum sollte die Nutzung von „Disaster Recovery as a Service“ in der Cloud geprüft werden.

„*Das weiß unser Admin doch*“ ist kein Wiederherstellungsplan!

Empfehlungen zu den IT-Plänen
Wiederanlauf (WAP) & Wiederherstellung (WHP)

- Achten Sie darauf, dass die **WHP hinreichend detailliert** beschrieben werden! Hinreichend bedeutet: Kann auch eine andere „IT-fachkundige Person“ ungleich dem eigentlichen Experten durchführen!
- Denken Sie daran, **Wiederanlauf- und Wiederherstellungspläne**, sowie **Notfallaccounts & Passwörter** für alle relevanten Systeme **ausgedruckt und gesichert aufzubewahren** – und diese Liste regelmäßig zu aktualisieren!

Gängige BCM-Tests

Schreibtischübungen: Durchgehen ausgewählter Szenarien zur Validierung der Notfallpläne

→ Uneingeschränkt empfehlenswert!

Technische Tests: Überprüfen von redundanten Infrastrukturen (z.B. Server, Stromversorgung etc.)

→ Falls vorhanden und relevant!

Simulation von Szenarien: Realistisches Üben eines Notfalls unter realistischen Bedingungen

→ Empfehlenswert, aber hoher Aufwand!

Ernstfall- oder Vollübung: Üben eines realistischen Ereignisgeschehens.

→ nicht empfehlenswert, falls nicht gefordert!

Üben und testen!

- Nutzen Sie die Übungen, um gleichzeitig die Unterlagen zu **aktualisieren!**
- Lassen Sie **nicht die Experten testen**, die die Pläne selbst geschrieben haben!
- Prüfen Sie zunächst auf dem **Papier**, ob die Planung mit allen Abhängigkeiten und Kausalitäten „so“ funktionieren kann!
- Gehen Sie in der IT gestuft vor:
  - Prüfen Sie, ob Ihre Backup-Wiederherstellung wirklich funktioniert!
  - Testen Sie die Wiederherstellung von Anwendungen/IT-Systemen!

Gerne helfen wir Ihnen bei Fragen weiter!

Scio GmbH

Ganzheitlicher Ansatz | Strategische Herangehensweise und Geschäftsprozessmanagement-Know How intelligent gekoppelt

Resultatorientierung | Konzepterstellung ist nicht unsere „definition of done“, Implementierung und Verankerung ist Teil unserer Mission

Gemeinsame Verantwortung | Formen und Empowern eines Teams, das die interne Unternehmensentwicklung vorantreibt

Streben nach Effektivität und Effizienz | Die richtigen Dinge richtig tun

Responsefähigkeit zählt | Unterschiedlicher Kontext benötigt unterschiedliche Ansätze und Tools, um sie optimal zu unterstützen

Freundlich und bodenständig | Eine produktive und angenehme Atmosphäre und unser Teamgeist trägt zu wertschöpfenden Ergebnissen bei

Markus Wolff

M.Sc. Informatik:
International Software Systems Science

Markus Wolff ist IT-Security-Berater und Softwarearchitekt bei Scio. Er befasst sich seit mehr als 15 Jahren mit Themen rund um Informations-/IT-Sicherheit, Softwarearchitektur und Cloud-Technologien.

Frank Büttner

Dipl. Wirtschaftsinformatiker

ist Geschäftsführer der Scio GmbH und verfügt über mehr als 18 Jahre relevante Beratungserfahrung. Seine Schwerpunkte liegen im Strategischen Management, dem Management komplexer Reorganisationsprojekte sowie im CIO-Advisory.

Sie haben Fragen oder wünschen sich Unterstützung?

Frank Büttner
Dipl. Wirtschaftsinformatiker (univ.)

Geschäftsführer

Telefon: 09131 530 2162
Mail / MS Teams / LinkedIn:
frank.buettner@scio.eu

Markus Wolff
M.Sc. Informatik: International Software Systems Science

IT-Security Berater

Telefon: 09131 5302161
Mail / MS Teams: markus.wolff@scio.eu