GRC Partner
Governance Risk & Compliance

(IT) Notfallmanagement im Unternehmen und in der Behörde

Planung und Umsetzung gemäß BSI-Standard 100-4 und ISO 22301

Smart Compliance Solutions

Agenda

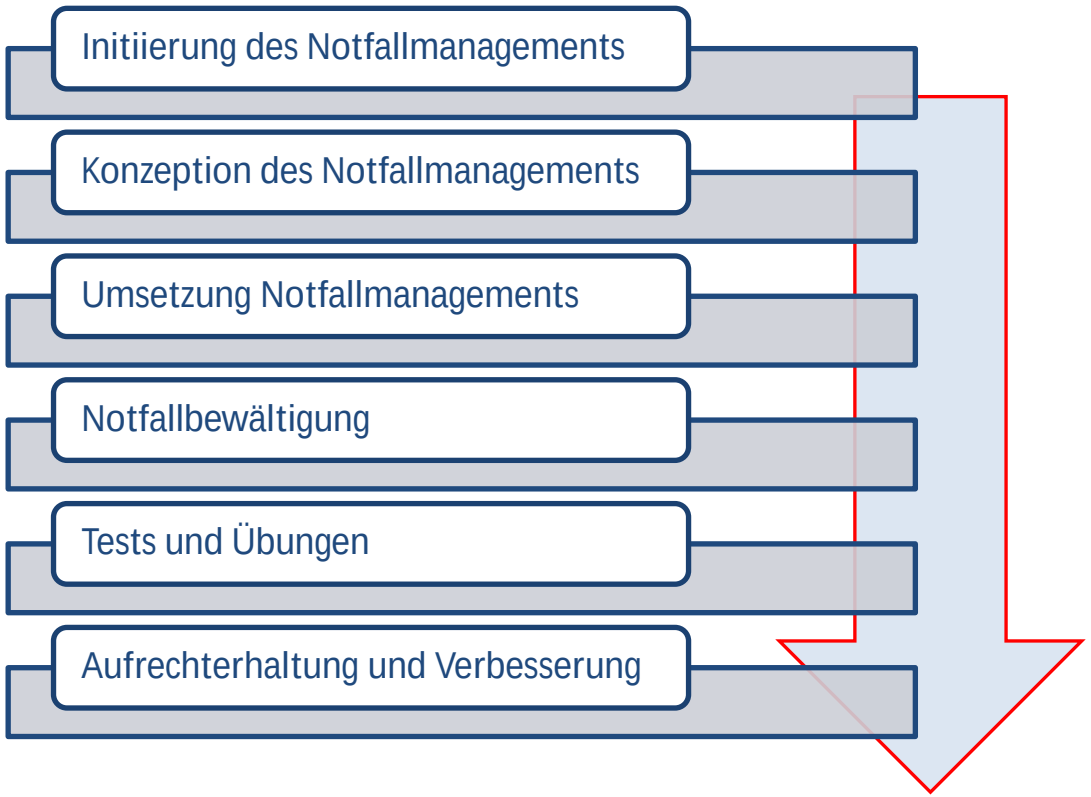
1. Definition des Notfallmanagements
2. Notfallmanagementprozess
3. Häufige Probleme bei der Umsetzung des Notfallmanagements

GRC Partner
Governance Risk & Compliance

Notfallmanagement

Definition:

§ *„Notfallmanagement ist ein **Managementprozess** mit dem Ziel, gravierende Risiken für eine Institution, die das Überleben gefährden, frühzeitig zu erkennen und Maßnahmen dagegen zu etablieren“* (*)

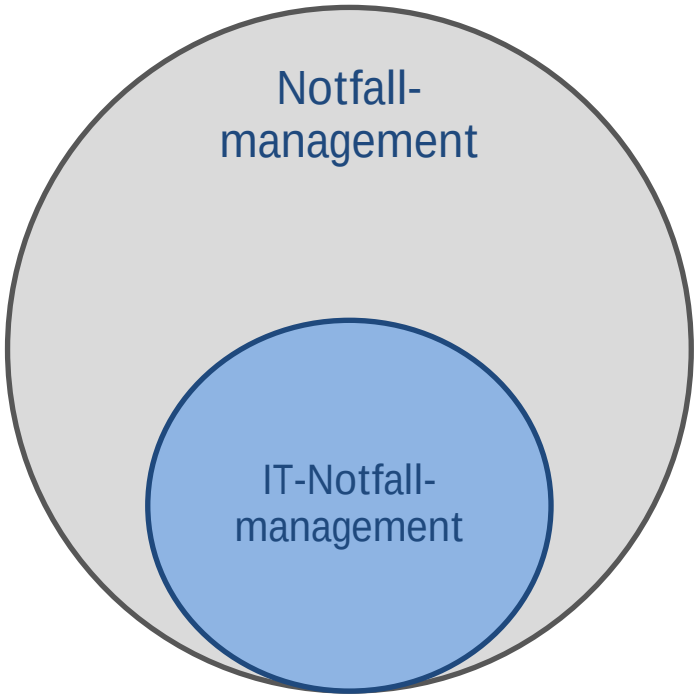


(*) ***Quelle: BSI***

GRC Partner
Governance Risk & Compliance

Begriffe:

- Begriffe „*Notfallmanagement*“, „*Business Continuity Management*“ und „*betriebliches Kontinuitätsmanagement*“ sind **gleichzusetzen** (*)
- *IT-Notfallmanagement* **ist ein Teil** des *Notfallmanagements* (*)



(*) ***Quelle: BSI***

GRC Partner
Governance Risk & Compliance

Notfallmanagementprozess

Zusammenfassung des Notfallmanagementprozesses:

- § Leitlinie und Verantwortlichkeiten
- § Notfallorganisation (Team-Bildung)

- § BIA
- § RIA (BSI-Standard 100-3, ISO 27005)
- § Soll-Ist- und Kosten-Nutzen-Analyse

- § Planung, Budgetierung, Ressourcen
- § Kontrolle der Umsetzung

- § Notfallhandbücher
- § Meldung, Alarmierung und Eskalation
- § Geschäftsfortführung und Wiederanlauf

- § Funktionstests, Simulation, Vollübung
- § Übungshandbuch

- § Interne Audits
- § Externe Audits

GRC Partner
Governance Risk & Compliance

Notfallmanagementprozess

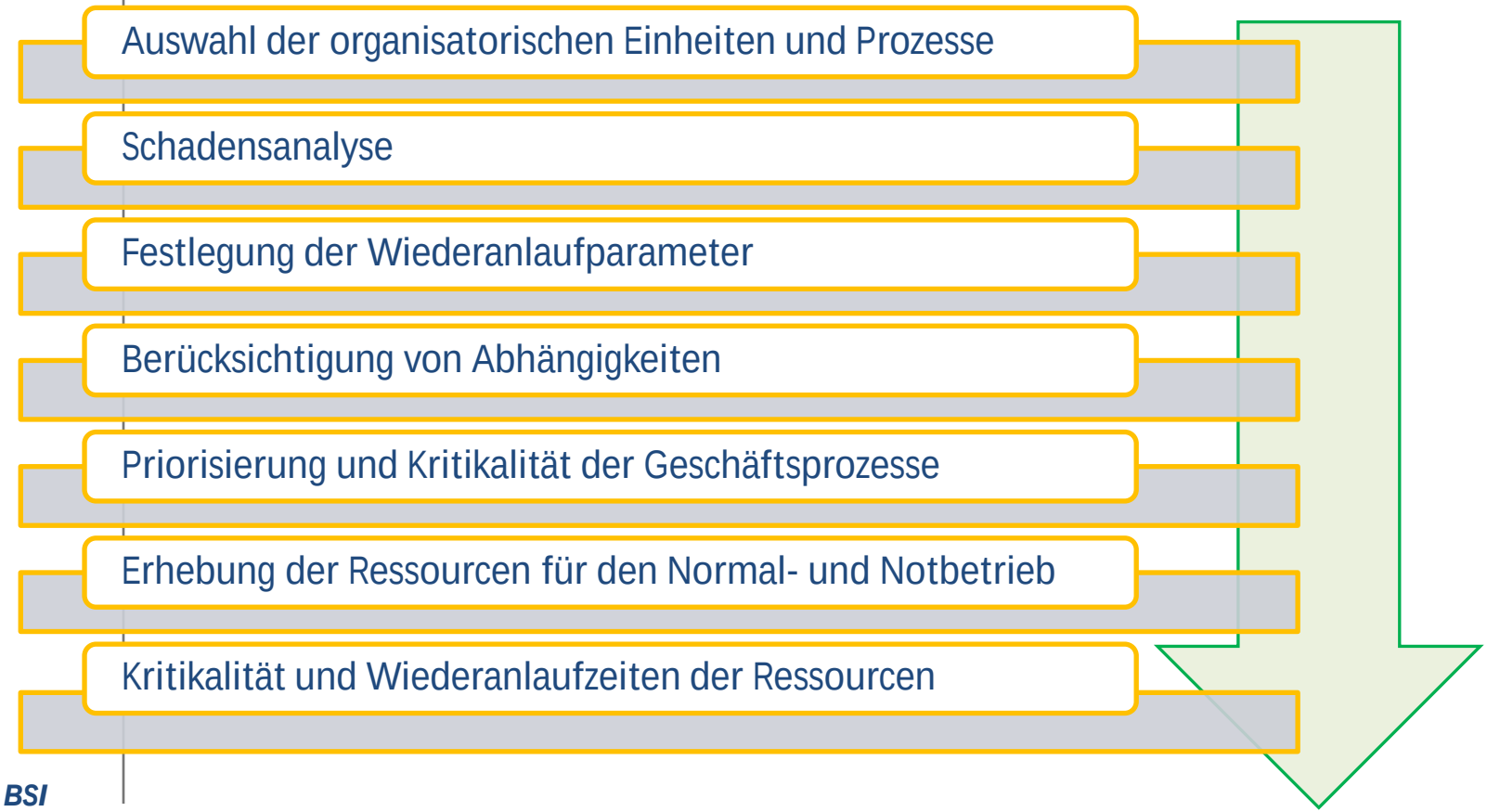
Häufige Probleme bei der Umsetzung (Auszug):

- Übernahme der Verantwortung durch die Leitungsebene
- Dokumentation der Organisation, Prozesse und IT
- Planung und Durchführung der BIA
  - Auswahl der organisatorischen Einheiten und Prozesse
  - Festlegung der Wiederanlaufparameter
  - Erhebung der Ressourcen für den Normal- und Notbetrieb
- Kontinuitätsstrategie (Kosten-Nutzen-Analyse)
- Tests und Übungen
- Dokumentation des Notfallmanagements mit MS Office Word und Excel

GRC Partner
Governance Risk & Compliance

Notfallmanagement [BIA-Prozess]

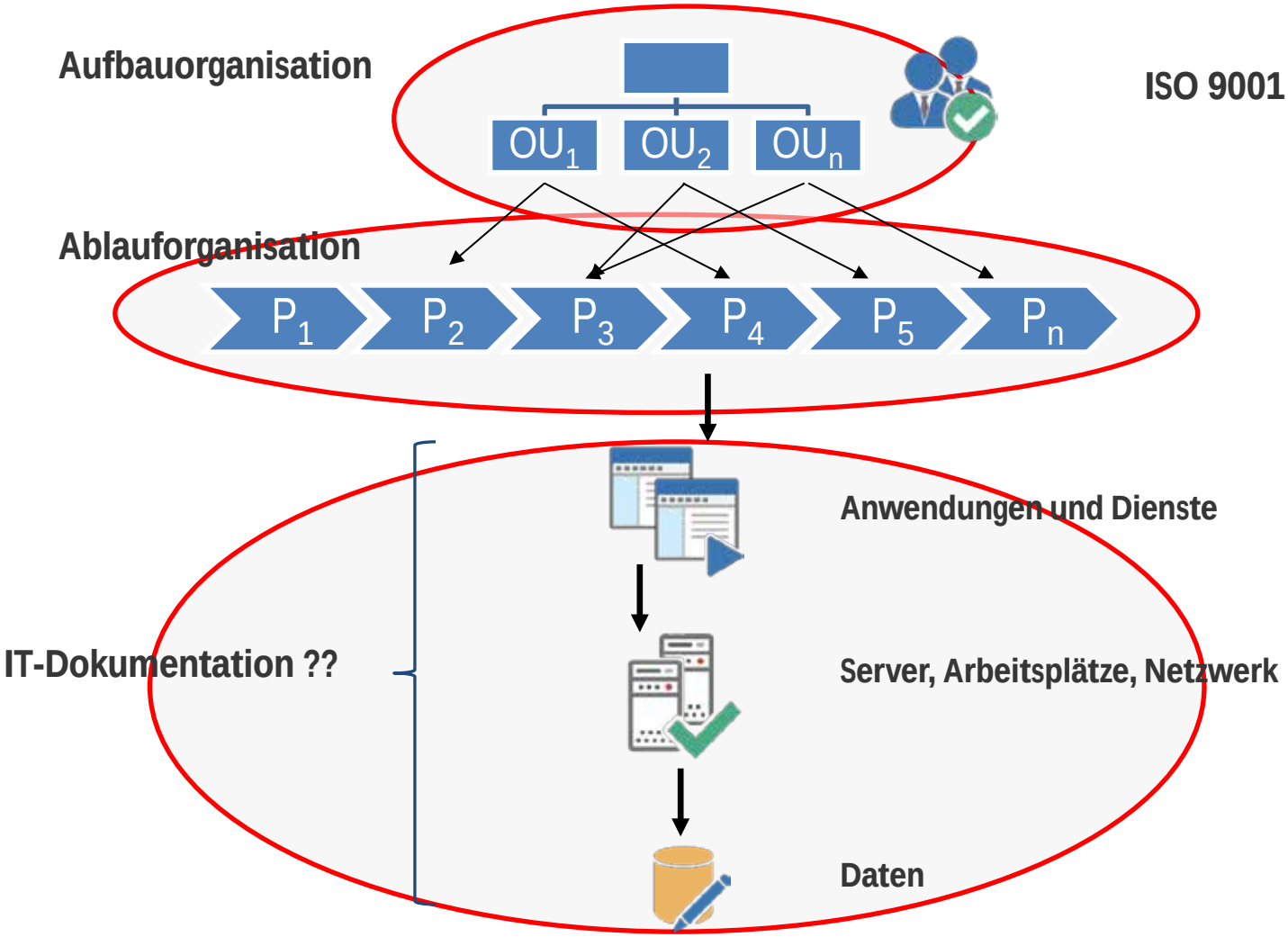
Business Impact Analyse - Prozess:



(*) ***Quelle: BSI***

GRC Partner
Governance Risk & Compliance

Welche Informationen werden für die BIA benötigt?



Auswahl der OE und Prozesse nach BSI-Standard 100-4:

Hinweis1: *„Ist **offensichtlich**, dass innerhalb des festgelegten Geltungsbereichs des Notfallmanagements Organisationseinheiten oder Geschäftsprozesse existieren, welche eine sehr geringe Kritikalität für die Institution besitzen, **so können diese bei der weiteren Betrachtung ausgespart werden**."*

Hinweis 2: *„Als allgemeine **Faustregel** kann gelten, dass das Ergebnis der Prozesserhebung in einer Organisationseinheit für das Notfallmanagement **5 bis maximal 15** Prozesse liefern sollte. Dies hat sich in der Praxis als sinnvoll erwiesen, kann jedoch institutions- und aufgabenabhängig durchaus unter- bzw. überschritten werden."*

**Wie kann vor dem BIA-Prozess festgestellt werden,
welche der Prozesse aus der Sicht des Notfallmanagements irrelevant sind?**

(*) ***Quelle: BSI-Standard 100-4, 5.1.2.1 Stammdaten und Geschäftsprozesse, S. 32 und S. 33***

GRC Partner
Governance Risk & Compliance

Beispielmethoden für die Auswahl der organisatorischen Einheiten und Prozesse für den BIA-Prozess:

M1. Es werden alle Prozesse und organisatorischen Einheiten aus dem Geltungsbereich des Notfallmanagements in die BIA einbezogen

M2. Betrachtung der betriebswirtschaftlichen Bedeutung der Prozesse

M3. Durchführung der ABC-Analyse

M4. Betrachtung der IT-Dienste oder Anwendungen

M5. Berücksichtigung der Compliance-Aspekte

Methode 1: Alle Prozesse und OE in der BIA-Betrachtung

- **Vorteile**
  - Als Ergebnis stehen detaillierte Informationen über alle organisatorischen Einheiten und Prozesse zur Verfügung
  - Abhängigkeiten und gegenseitige Wechselwirkungen der Prozesse sind bestens bekannt

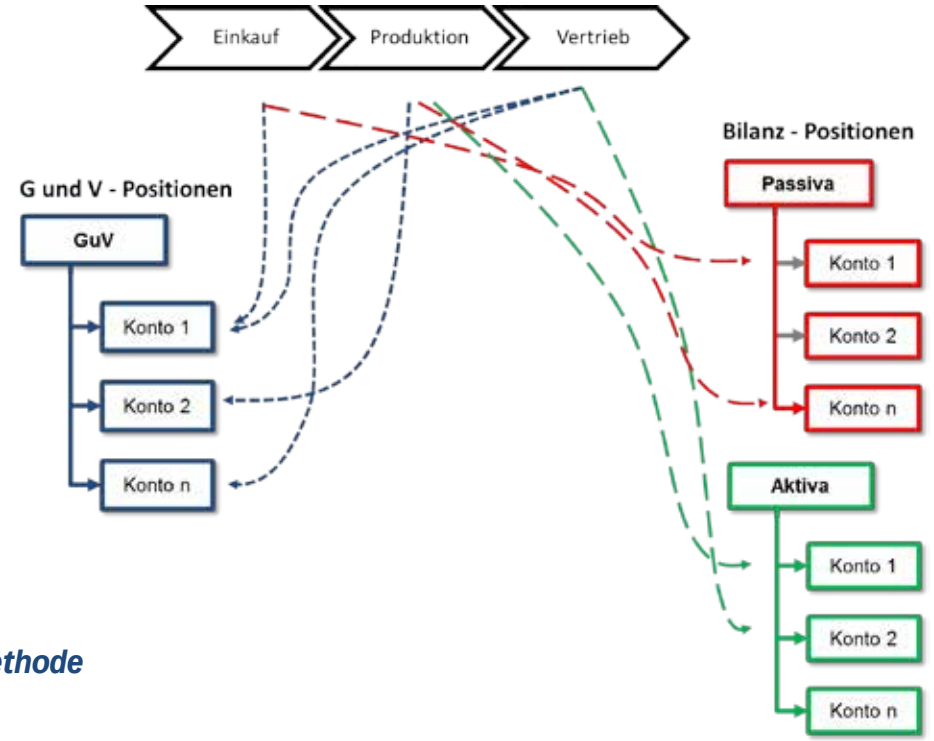
- **Nachteile**
  - Es kann sehr zeitaufwendig und somit kostspielig sein
  - Für die Durchführung der BIA werden überdurchschnittlich viele Ressourcen benötigt
  - Kein Vorteil gegenüber alternativen Methoden

Die Methode ist nicht empfehlenswert!

GRC Partner
Governance Risk & Compliance

Methode 2: Betriebswirtschaftliche Bedeutung der Prozesse

- **Ausgangspunkt** der Auswahl ist die Analyse der Prozesse und der **Bilanz- /G und V**-Positionen, in denen sie münden (*)
- Festlegung der **Wesentlichkeitsgrenze (ein Betrag)**



(*) ***IKS Methode***

Methode 2: Betriebswirtschaftliche Bedeutung der Prozesse

- **Vorteile**
  - Die Anzahl der einbezogenen Prozesse kann signifikant eingeschränkt werden
  - Effiziente und effektive Durchführung der BIA
  - Handfeste Begründung für die Auswahl der Prozesse

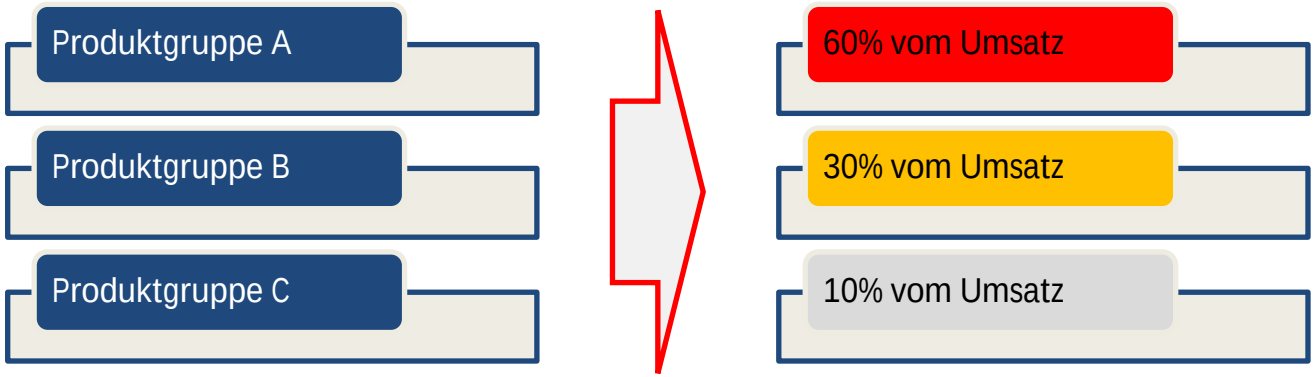
- **Nachteile**
  - Nicht alle Prozesse münden direkt in den Bilanz- /G und V-Positionen, trotzdem können sie für die Leistungserstellung der Organisation unabdingbar sein
  - Methode berücksichtigt die Compliance-Aspekte, wie z.B. Umweltschutz- und Steuer-Gesetze oder Verträge mit den Geschäftspartnern nicht

Die Methode ist empfehlenswert!

GRC Partner
Governance Risk & Compliance

Methode 3: ABC-Analyse

- Betrachtung der Wertschöpfungskette
  - Nutzung der **Kennzahlen** aus dem Controlling
  - Gruppierung der Leistungen bzw. **Produkte** in A-B-C Kategorien nach dem generierten **Umsatz**
  - Häufig liefert eine **kleine Anzahl** der Produkte den **wesentlichen Wertbeitrag** für ein Unternehmen ***(Paretoprinzip)***
  - Aus den Ergebnissen werden die systemrelevanten OE und Prozesse abgeleitet



GRC Partner
Governance Risk & Compliance

Methode 3: ABC-Analyse

- **Vorteile**
  - Die Anzahl der einbezogenen Prozesse kann signifikant eingeschränkt werden
  - Effiziente und effektive Durchführung der BIA
  - Handfeste Begründung für die Auswahl der Prozesse

- **Nachteile**
  - Nicht alle Prozesse liefern einen direkten Beitrag zum Umsatz
  - In einigen Prozessen können Produkte aus mehreren Produktgruppen, wie z.B. A und C produziert werden
  - Methode berücksichtigt die **Compliance-Aspekte**, wie z.B. Umweltschutz- und Steuer-Gesetze oder Verträge mit den Geschäftspartnern nicht

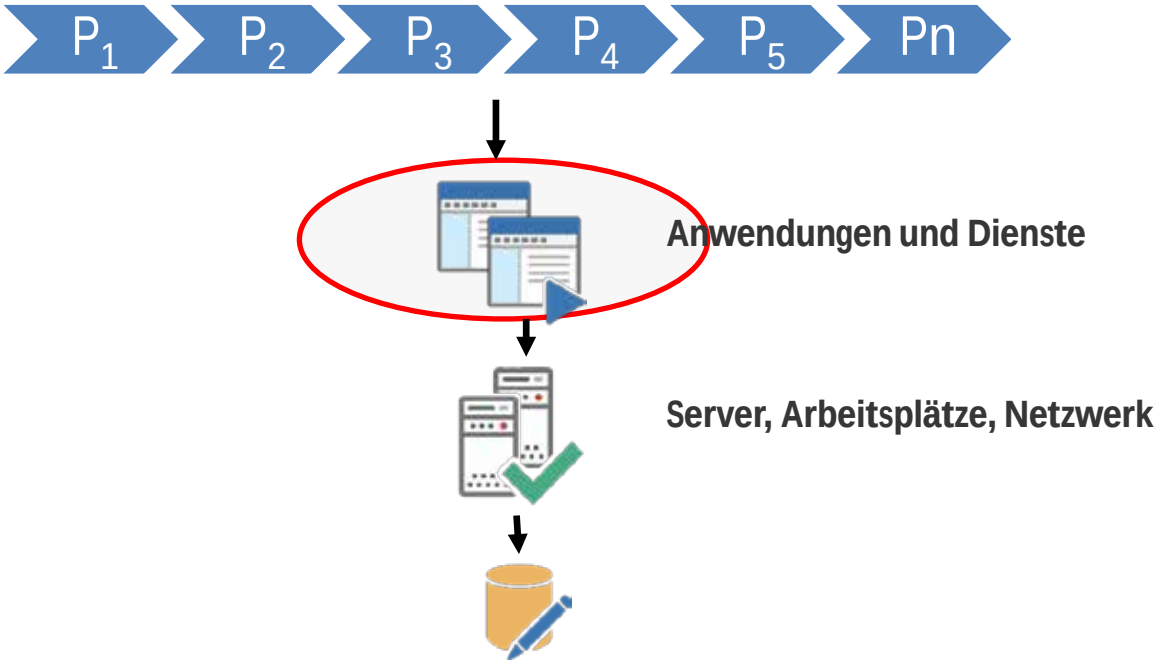
Die Methode ist empfehlenswert!

GRC Partner
Governance Risk & Compliance

Methode 4: Betrachtung der Anwendungen oder Dienste

- Nutzung der Tatsache, dass wenige aber sehr kritische Anwendungen, wie z.B. ERP einen Großteil der Geschäftsprozesse bedienen

- Anstatt einzelne Prozesse, wie z.B. Beschaffung, Produktion, Buchhaltung etc. in der BIA zu betrachten, wird die ERP-Anwendung stellvertretend für die genannten Prozesse analysiert.



GRC Partner
Governance Risk & Compliance

Methode 4: Betrachtung der Anwendungen oder Dienste

- **Vorteile**
  - Es werden nur Anwendungen und /oder Dienste betrachtet
  - Effiziente und effektive Durchführung der BIA
- **Nachteile**
  - Weitere einzelne Anwendungen, wie z.B. Schnittstellen müssen berücksichtigt werden
  - Die Wiederanlaufparameter, wie z.B. MTA und WAZ können nur für die Anwendung und nicht für einzelne Prozesse festgelegt werden

Die Methode ist empfehlenswert!

Methode 5: Betrachtung der Compliance-Aspekte

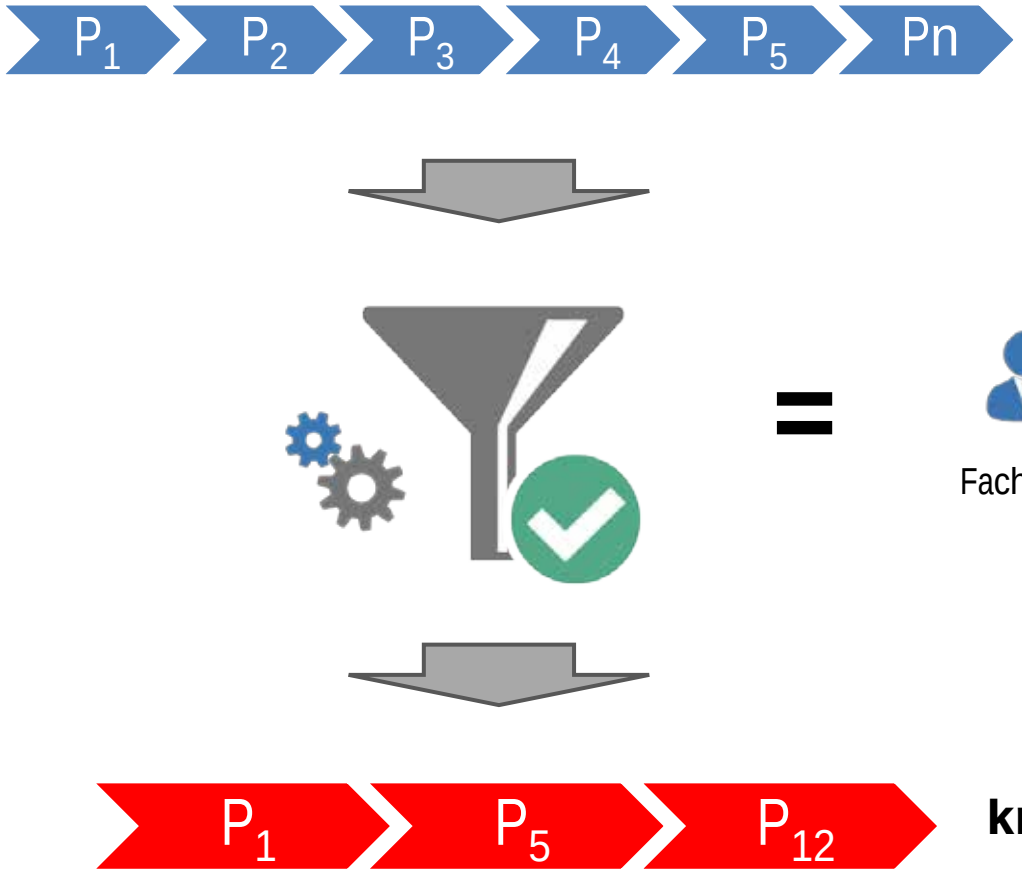
- Berücksichtigung aller Prozesse, deren Verfügbarkeit einen direkten Einfluss auf die **Erfüllung der geltenden** Gesetze haben können
  - **Branchenunabhängige** Gesetze, wie z.B. Umwelt- oder Steuergesetze
  - **Branchenabhängige** Gesetze, wie z.B. MaRisk, StrlSchV, SeeEigensichV
- Berücksichtigung von Prozessen **ohne besondere wirtschaftliche Bedeutung**
- Diese Methode hat keine **Vor-** und **Nachteile**,

  sie ist auch **keine Option sondern ein „Muss“**

Die Methode ist empfehlenswert!

GRC Partner
Governance Risk & Compliance

Das Ergebnis der Business Impact Analyse:



GRC Partner
Governance Risk & Compliance

Vgl. „(IT) Notfallmanagement im Unternehmen und in der Behörde“ - Kapitel 7.12.3 „Vorgang 2 – Business Impact Analyse“

Vielen Dank für Ihre Aufmerksamkeit

DocSetMinder®
Ready for Audit

Krzysztof Paschke
Geschäftsführer und Berater

GRC Partner GmbH
Bollhörnkai 1 Ÿ D-24103 Kiel
Ein Unternehmen der AKRA Gruppe

kpaschke@grc-partner.de
+49 431 530 33 990

GRC Partner
Governance Risk & Compliance