Mit der NIS-Kanne durchs Unternehmen?

Umsetzung der NIS2 Maßnahmen aus Sicht eines kritischen Infrastrukturbetreibers

Ing. Wolfgang Löw, MSc | Ing. Dr. Alexander Novotny, MSc
IT-SECX 2024, FH St. Pölten

Vorstellung

Ing. Wolfgang Löw, MSc

- CISO EVN Konzern
- Mitglied Board of Directors des EE-ISAC

Ing. Dr. Alexander Novotny, MSc, BSc

- Local Security Officer EVN Konzern-IT
- Schwerpunkte Risikomanagement & Governance

Agenda

- NIS 2 Einführung
- NIS2 in der EVN Gruppe
- Vorstellung Risiko-basierte Vorgehensweise
- Best Practice Learnings

Bildnachweis: Abbildungen wurden mit Microsoft Bing Image Creator erstellt

NIS 2 Einführung

→ NIS2 Richtlinie

- Inkrafttreten mit 16.1.2023 – Überführung in nationales Gesetz durch bis 17.10.2024
- Harmonisierung Anwendungsbereich, Sicherheitsmaßnahmen, Meldepflichten
- Anwendungsbereich von NIS-2 umfasst 18 Sektoren
- Entfall des wesentlichen Dienstes – Unterscheidung in wesentliche und wichtige Einrichtungen
- Erhöhter Strafrahmen

Ein riesiger Garten, aber nur begrenzte Gärtner und Ressourcen für die Bewässerung?

Unser Garten ist größer als Niederösterreich

- NIS2 in (Nieder-)österreich, Bulgarien und Kroatien; nationales Cybersicherheitsgesetz in Nord-Mazedonien
- Mehrere hundert Geschäftstätigkeiten müssen bewertet werden
- Über hundert IT/OT Services müssen analysiert werden
- Mehrere Dutzend IT/OT Services haben einen erweiterten oder hohen Schutzbedarf

Ziele

Standardisierte Vergleichbarkeit in der gesamten EVN Gruppe

Hohe Effizienz der Umsetzung

Risikobasiertes Vorgehen nach drei Schutzbedarfs-Stufen

Gießkanne

→ Standard-Maßnahmen

Erhöhte Pflege

→ Erweiterte Maßnahmen

Individuelle Pflege im Glashaus

→ Engmaschige Maßnahmen

Relevante IT/OT-Services werden anhand der Auswirkungen aus den Geschäftstätigkeiten erhoben, um Diese nachfolgend bewerten zu können

Schritt 1

Erhebung der Geschäftstätigkeiten

Evaluierung aller Geschäftstätigkeiten in Zusammenarbeit der jeweiligen Fachabteilung

Ziel:
Finden aller Geschäftstätigkeiten und bewerten der Geschäftstätigkeiten nach Auswirkungsgrad

Schritt 2

Business Impact Analyse (BIA)

Durchführung der BIA durch Beantwortung der Leitfragen

Ziel:
Analysieren und bewerten von Geschäftstätigkeiten **ab einer mittleren Auswirkung** und bestimmen der benötigten IT/OT Services.

Schritt 3

GAP-Analyse einzelner IT/OT Services

Durchführung der GAP-Analyse bzw. Schutzbedarfsfeststellung der IT/OT-Services mit relevanter Auswirkung.

Ziel:
Finden von Abweichungen in den IT/OT-Services mit relevanter Auswirkung, zur Ableitung notwendiger Maßnahmen.

Schema: Ablauf der BIA

Erhebung aller Geschäftstätigkeiten

Vorbewertung

Schutzbedarf: mittel, hoch oder sehr hoch

Detaillierte BIA für Schutzziele mit Vorbewertung > gering

Erhebung der IT/OT Services

Durchführung detaillierter BIA für **notwendige** IT/OT Services

Schutzbedarf: unbedeutend oder gering

unterstützendes IT/OT Service

Schutzbedarf IT/OT Service unbedeutend oder gering

Schutzbedarf IT/OT Service mittel oder hoch

Schutzbedarf IT/OT Service sehr hoch

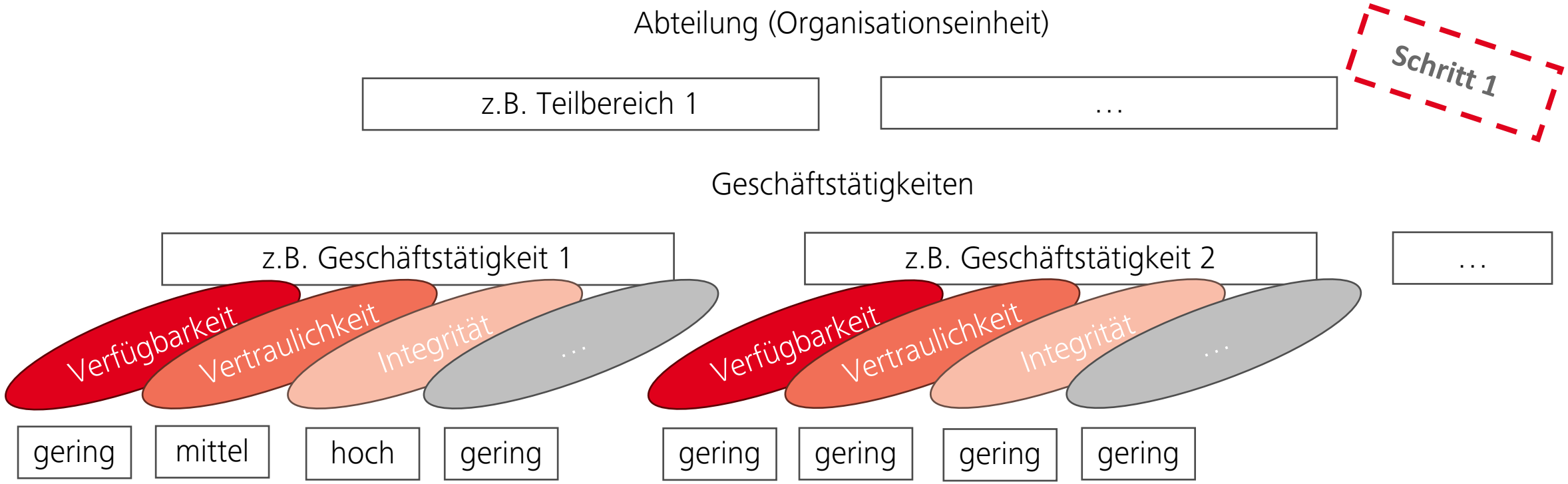
„Basisschutz“

„erweiterter Schutz“

„hoher Schutz“

Schritt 1: Welche Pflanzen wachsen im Garten und welche davon sind empfindlich?

Schritt 1: Erhebung der Geschäftstätigkeiten



→ Erfassen der Geschäftstätigkeiten in der Organisationseinheit

→ Vorbewertung in Schritt 1 (reduzierte Fragen)

→ Quality Gate: Geschäftsführung genehmigt Vorbewertung und priorisiert

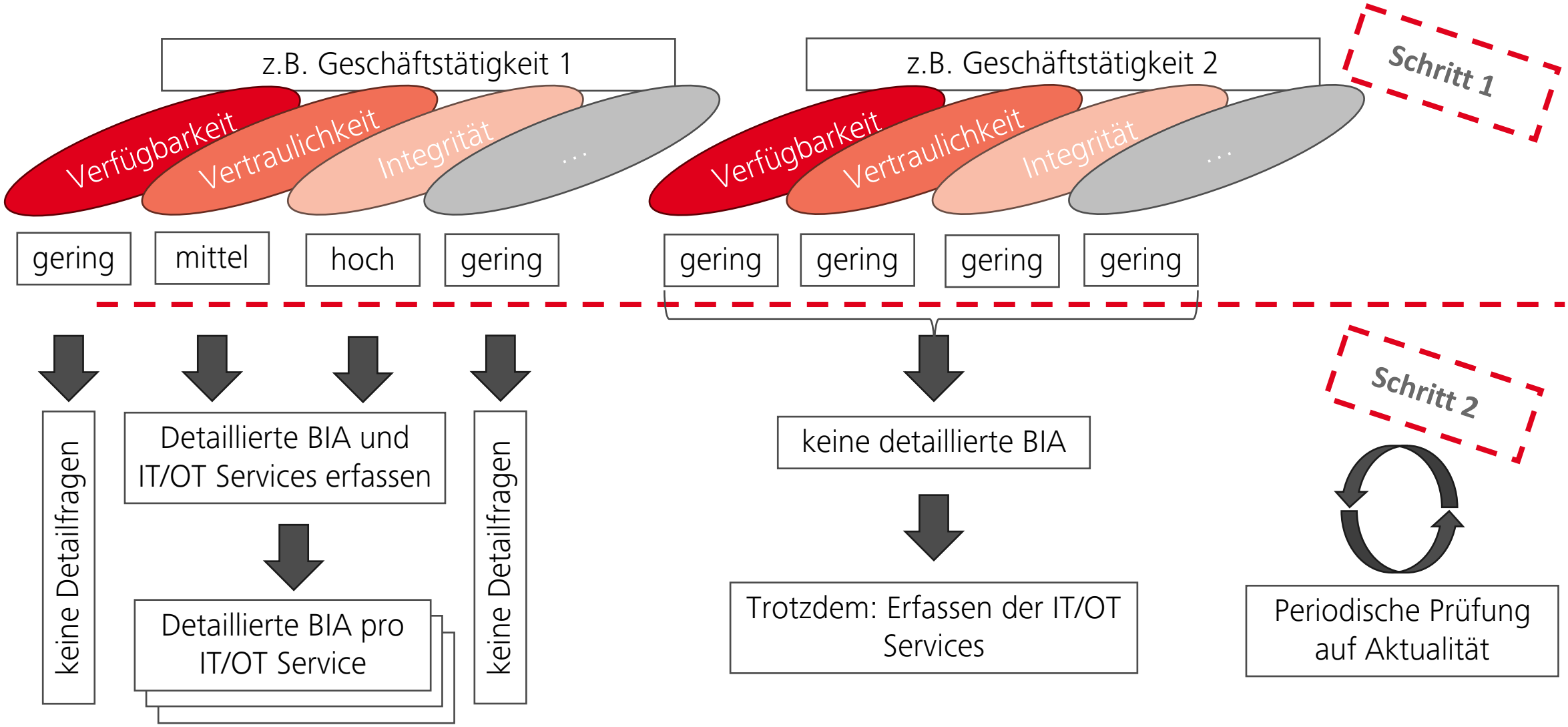
Schritt 2: Was passiert, wenn eine Pflanze krank wird oder zu wenig/viel Wasser bekommt?

Zu viel oder zu wenig Pflege?

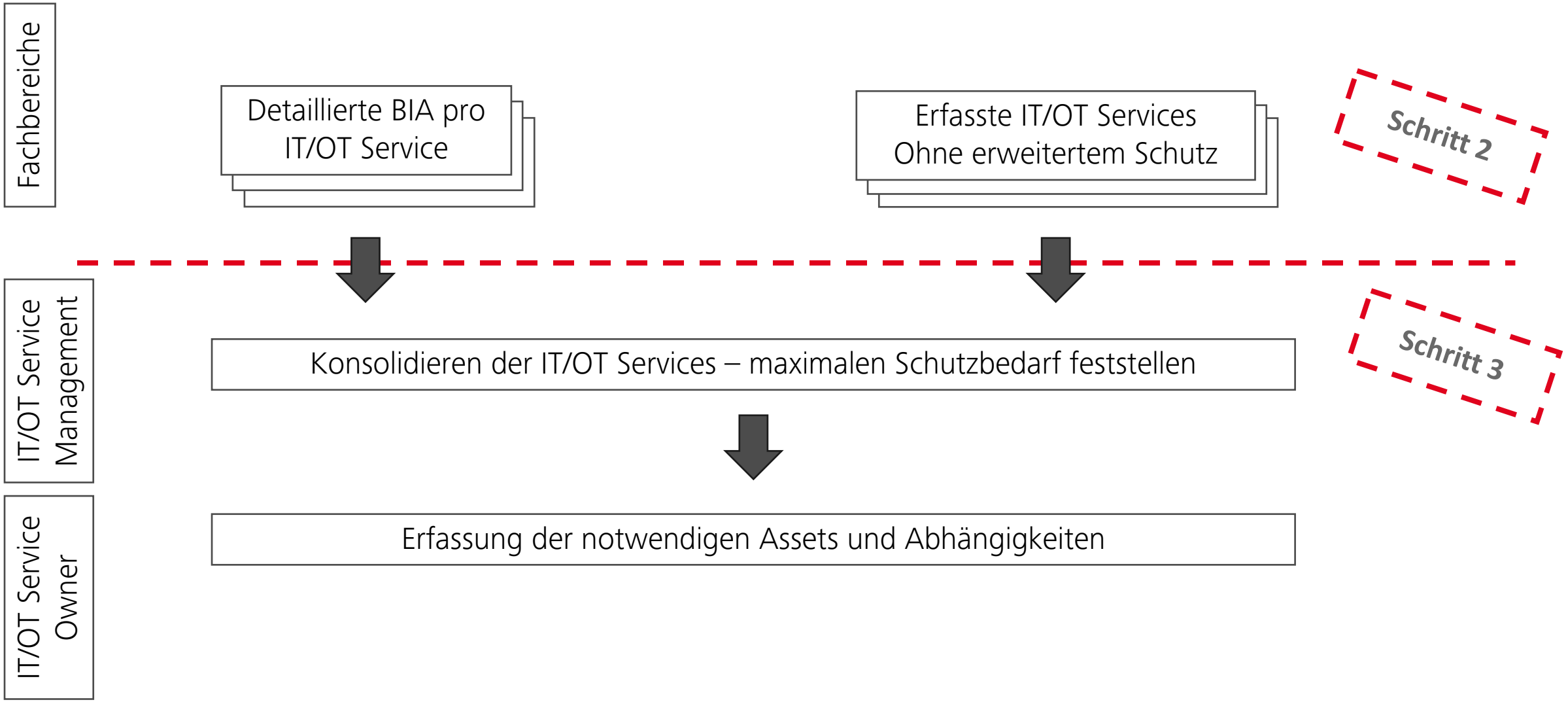
→ Angemessene Sicherheitsmaßnahmen für jedes IT/OT Service

→ Security soll ein Business Enabler sein und keine Innovationen verhindern

Schritt 2: weiterführende BIA durchführen



Schritt 3: IT/OT Services nach dem Maximalprinzip konsolidieren



Schritt 3: GAP-Analyse einzelner IT/OT Services

Warum?

→ Finden relevanter Abweichungen zu

– gesetzlichen Vorgaben (NIS 2, CRA, CRE, …) und Normvorgaben (ISO27001, …)

– in den IT/OT-Services mit hoher Auswirkung

– zur Ableitung notwendiger Maßnahmen

Wer?

→ Bereiche, welche IT oder OT Services bereitstellen / betreiben

Herausforderungen

→ Gesetzliche Vorgaben (nationale NIS Verordnung) noch unklar

→ Orientierung an ISO 27001/ISO 27002/ISO 27019

Kernbotschaften / Best Practice Learnings

- → Management Unterstützung des gesamten Vorhabens
- → Management Priorisierung und Genehmigung
  - – nach Phase 1, welche Bereiche im Detail betrachten werden sollen
- → Frühe Involvierung der betroffenen Unternehmens-Bereiche + PoC und Lernphase
- → So einfach wie möglich, so detailliert wie nötig
- → Vorbereitung der durchführenden Personen
  - – Trainings für die Methode
  - – Leitfaden für Interviewführung → Vergleichbarkeit der Ergebnisse
- → Ressourcen-intensiv, Skalierung notwendig

Fragen und Antworten