iseco consulting

verinice.XP

RUN in verinice.PRO

Berlin, Donnerstag, 12.02.2026

Agenda

01	Begriffserklärungen
02	Ausgangslage
03	Ziel
04	Vorgangsweise
05	ISMS – Aufbau
06	Masterstandard

Um was geht es hier?

RUN – Lauf ISB, lauf…

RUN

- **R**eife- und **U**msetzungsgradbewertung im Rahmen der **N**achweisprüfung
- Bewertet
  - **Reifegrade** (ISMS/BCMS) und
  - **Umsetzungsgrade** für Detektion und Reaktion (SzA) und (OrgM, PerM, PhyM, TecM)

RUN Reife- und Umsetzungsgrade

- RUN definiert jeweils **fünf Reifegrade** und **fünf Umsetzungsgrade**, um die **Reife von Managementsystemen** und den **Umsetzungsstand von Maßnahmen** durch Prüfer bewerten zu lassen:

Nr	Reifegrad ISMS, BCMS	Umsetzungsgrad Einzelne Maßnahmenbereiche
1	Geplant	Ohne Maßnahmenumsetzung
2	Gesteuert	Einzelmaßnahmen, Teildurchführung
3	Etabliert	Maßnahmen umgesetzt, Prozessdurchführung
4	Messbar	Maßnahmen umgesetzt, plus Messbarkeit
5	Kontinuierlich verbessert	Maßnahmen umgesetzt, plus Verbesserung

Aber warum RUN(ning)?

Warum?

- Ziel der Anpassung ist es, die **Bewertung gesetzlicher Anforderungen** transparenter zu machen
- RUN-Reife- und Umsetzungsgrade helfen dabei, Handlungsbedarfe klar zu erkennen und gezielt weiterzuentwickeln: Niedrige Grade zeigen erhöhten Verbesserungsbedarf an
- Gleichzeitig sorgt die einheitliche Bewertungsmethode für eine **standardisierte und vergleichbare Nachweiserbringung** gegenüber dem BSI

Reicht denn RUN?

- Die RUN-Konkretisierung und die genannten Anforderungen sind nicht vollständig und keine alleinige Prüfungsgrundlage
- Individuelle Risiken müssen zusätzlich ermittelt und mit passenden Maßnahmen behandelt werden
- Branchen- und Sektorspezifika sind zwingend zu berücksichtigen
- Spezielle Anforderungen werden in Branchenspezifischen Sicherheitsstandards (B3S) abgebildet. B3S können – sofern vom BSI geeignet befunden – Ersatzmaßnahmen zulassen, wenn branchenspezifische Einschränkungen eine vollständige Umsetzung (z. B. der KdA) verhindern

GAiN – Is wat für den Prüfer

GAiN

- Das BSI legt in diesem Dokument verbindliche Anforderungen fest
- Jede Anforderung besitzt eine Kennung, die ihre Zuordnung erleichtert:
  - D = Durchführung
  - N = Nachweise
  - P = Prüfende Stelle
- Die Anforderungen sind thematisch strukturiert und decken unterschiedliche praktische Bereiche ab
- Themenbereiche werden in den Kennungen abgebildet, z. B. N.DG.01 für Dokumentation des Geltungsbereichs

KdA – Drill Down (kein Fracking, Donnie)

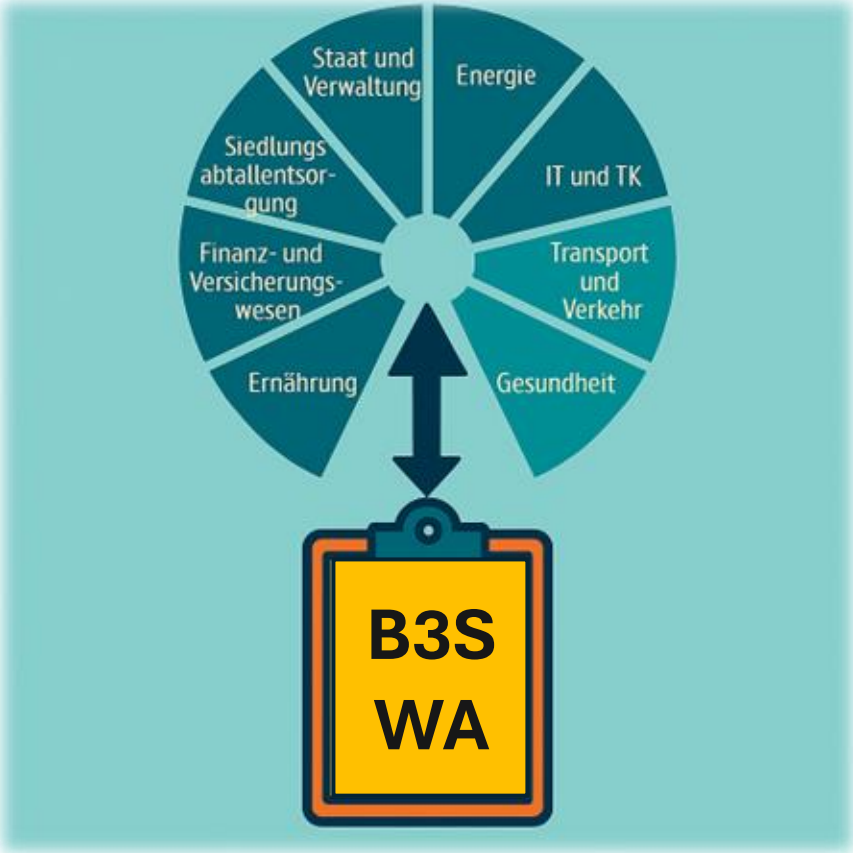
KdA

- Das Dokument konkretisiert die Anforderungen aus § 8a Abs. 1 und 1a BSIG für KRITIS-Betreiber und prüfende Stellen
- Es dient als Orientierung, um geeignete Sicherheitsvorkehrungen auszuwählen, umzusetzen und zu prüfen
- Der Katalog stellt Prüfkriterien für Nachweise nach § 8a Abs. 3 BSIG bereit
- Die Anforderungen sind nicht verbindlich und keine abschließende Prüfgrundlage – gleichwertige Alternativen sind möglich
- Individuelle Risiken müssen weiterhin eigenständig bewertet und mit Maßnahmen behandelt werden
- Branchenspezifische Besonderheiten sind zu berücksichtigen; hierfür existieren B3S-Standards, die auch Ersatzmaßnahmen definieren können, sofern vom BSI geeignet festgestellt

B3S WA – Und noch nen Standard?

B3S – Wasser/Abwasser

- Ein Branchenspezifischer Sicherheitsstandard (B3S) wird von einer Branche selbst entwickelt, um die Anforderungen aus § 8a BSIG praxisnah umzusetzen
- Er beschreibt branchentypische Sicherheitsanforderungen und Maßnahmen, die den Stand der Technik für eine bestimmte kritische Dienstleistung definieren
- B3S bieten KRITIS-Betreibern Orientierung bei der Auswahl und Umsetzung angemessener organisatorischer und technischer Sicherheitsmaßnahmen
- Sie schaffen Klarheit und Vergleichbarkeit, ohne neue gesetzliche Pflichten einzuführen
- Stattdessen konkretisieren sie bestehende Anforderungen branchenspezifisch, damit Betreiber diese effizient, nachvollziehbar und auditfähig erfüllen können
- Anwendungsfälle => Sammlung von BSI Anforderungen



Ausgangslage

Was haben wir vorgefunden

- Neue Prozessleittechnik
- ISMS als Teil der Ausschreibung
- Kleine IT mit Fokus Prozessleittechnik
- Office IT wird durch die Stadt verwaltet

- QMS implementiert

- ISMS/Regelwerk auf Basis 27001

Ziel

Vorgehensweise

Projektorganisation

- Vorbereitung
- Planung
- Festlegen der Geltungsbereiche

Vorgehen BSI Grundschutz/B3S

1. Strukturanalyse
   - Prozessanalyse & Dokumentation
   - Strukturanalyse & Dokumentation
2. Schutzbedarf
   - Kategorien
   - Feststellung
3. Modellierung
   - Bausteine nach Grundschutz
   - Anwendungsfälle B3S
4. Grundschutzcheck
   - Umsetzungsgrad der Anforderungen BSI Grundschutz
   - Mapping auf B3S
5. Risikoanalyse
   - B3S
   - BSI

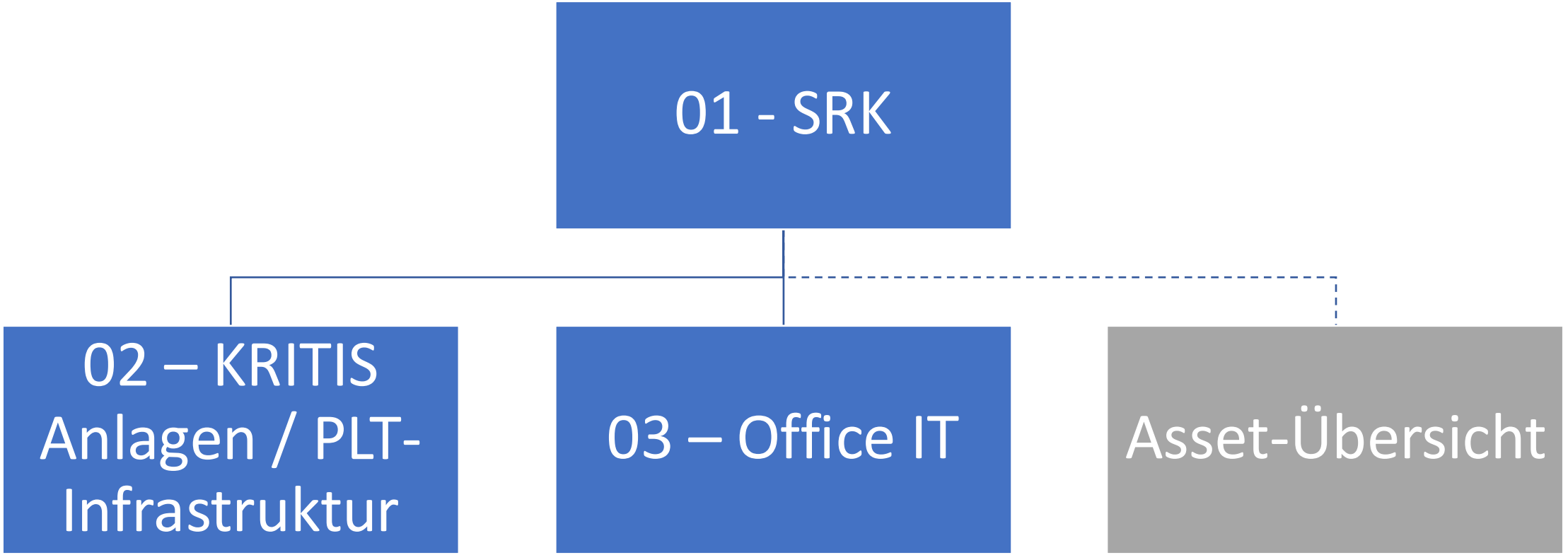
Leitlinie und Richtlinien

- ISMS-Organisation
- A 0 Dokumente A 1- A6 Doku
- Richtlinien aus den modellierten Bausteinen
- Toolarbeiten
- Dokumentation Prozessleitsystem
  - Systemdoku etc.

Umsetzungsphase

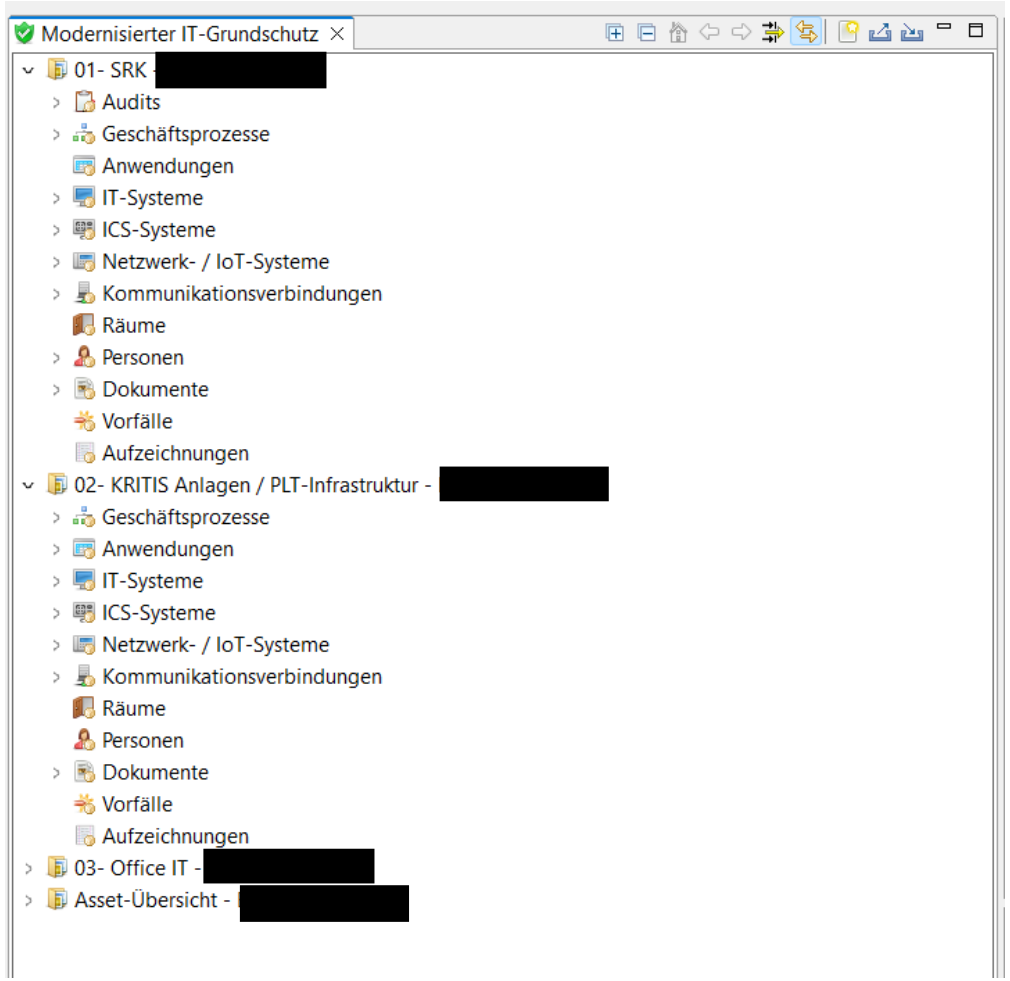
- Maßnahmenplanung und Umsetzung
- Internes Audit

ISMS - Aufbau


01 - SRK
02 – KRITIS Anlagen / PLT-Infrastruktur
03 – Office IT
Asset-Übersicht

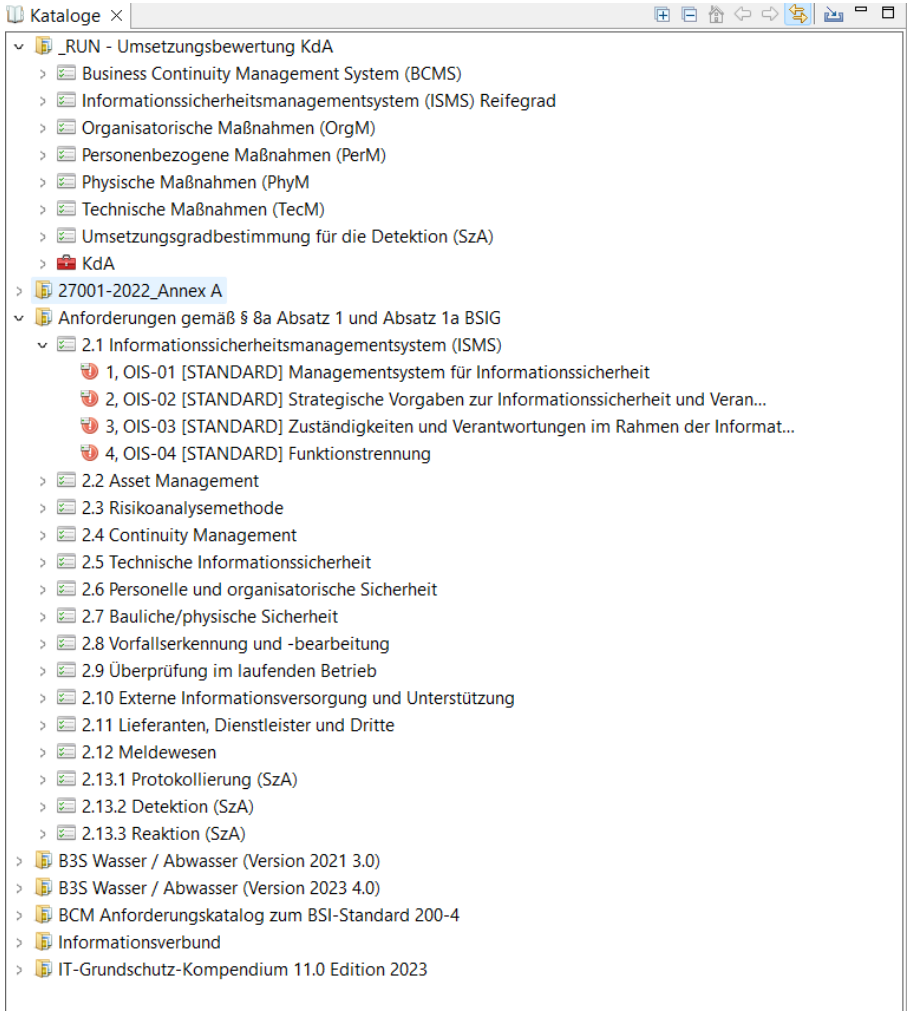
Vorstellung ISMS

- Abbildung der vier Informationsverbünde in dem ISMS-Tool verinice
- Alle Assets und Prozesse in verinice aufgenommen
- Verinice bildet die Grundlage für das ISMS des Kunden
- Referenzdokumente A.1 – A.6 direkt als Report aus verinice



Vorstellung ISMS

- Alle Anforderungen als Kataloge in verinice eingebunden
- Neben den Standards BSI-Grundschutz Kompendium und ISO 27001
  - RUN-Umsetzungsbewertung
  - Anforderungen gemäß § 8a BSIG
  - B3S Wasser / Abwasser
  - BCM Anforderungskatalog BSI 200-4



ISMS Dokumentation

- ISMS-Dokumentationsstruktur nach BSI-Grundschutz
- Auch zukünftig Grundschutz++ kompatibel
- Klarer Nachweis für jegliche Audits

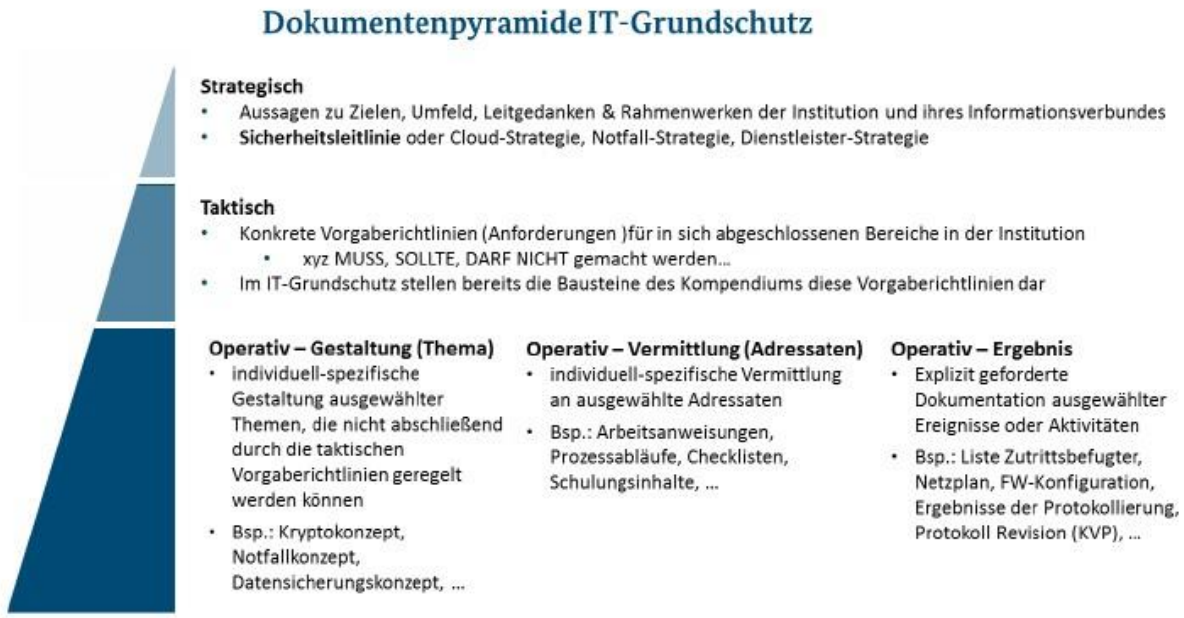
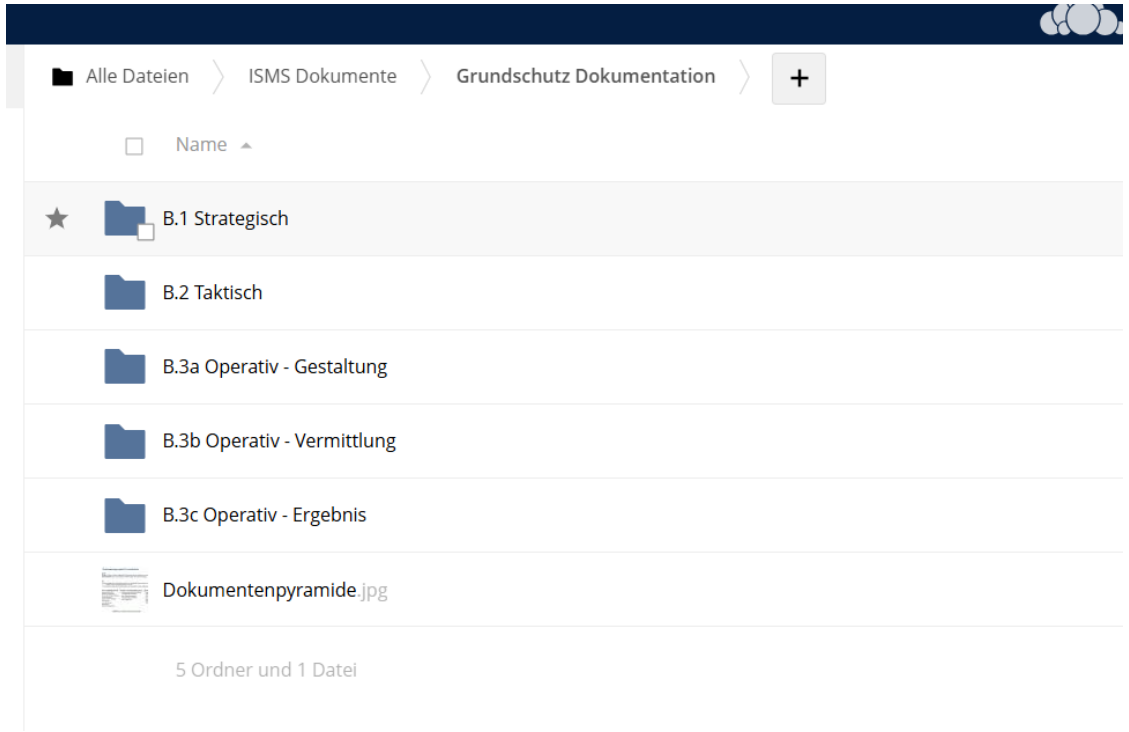


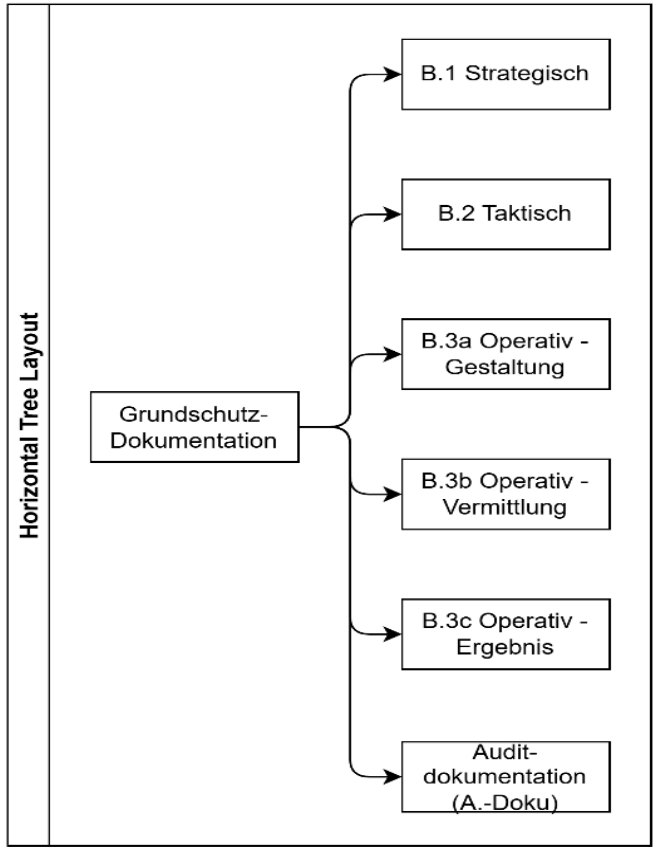
Abbildung 1: Dokumentationspyramide

ISMS Dokumentation

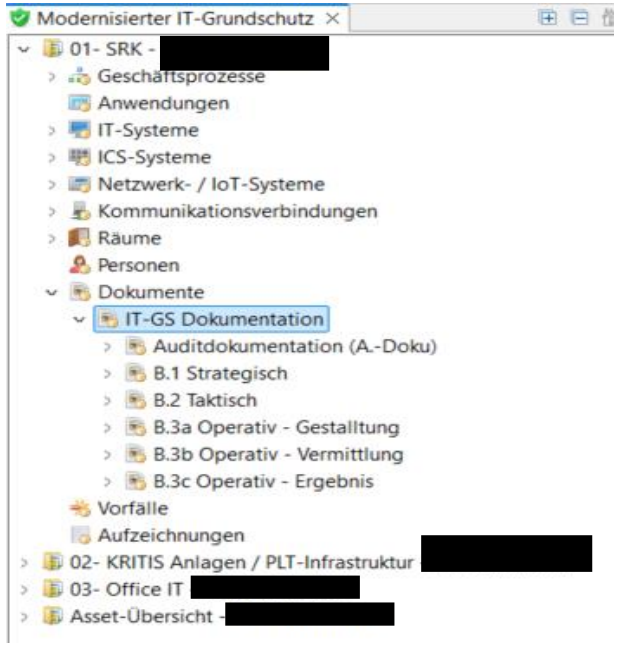
- Erstellte ISMS-Dokumente im Projekt
  - Strategische Dokumente 6
  - Taktische Dokumente 1
  - Operative Dokumente 34
- Ablageort ownCloud



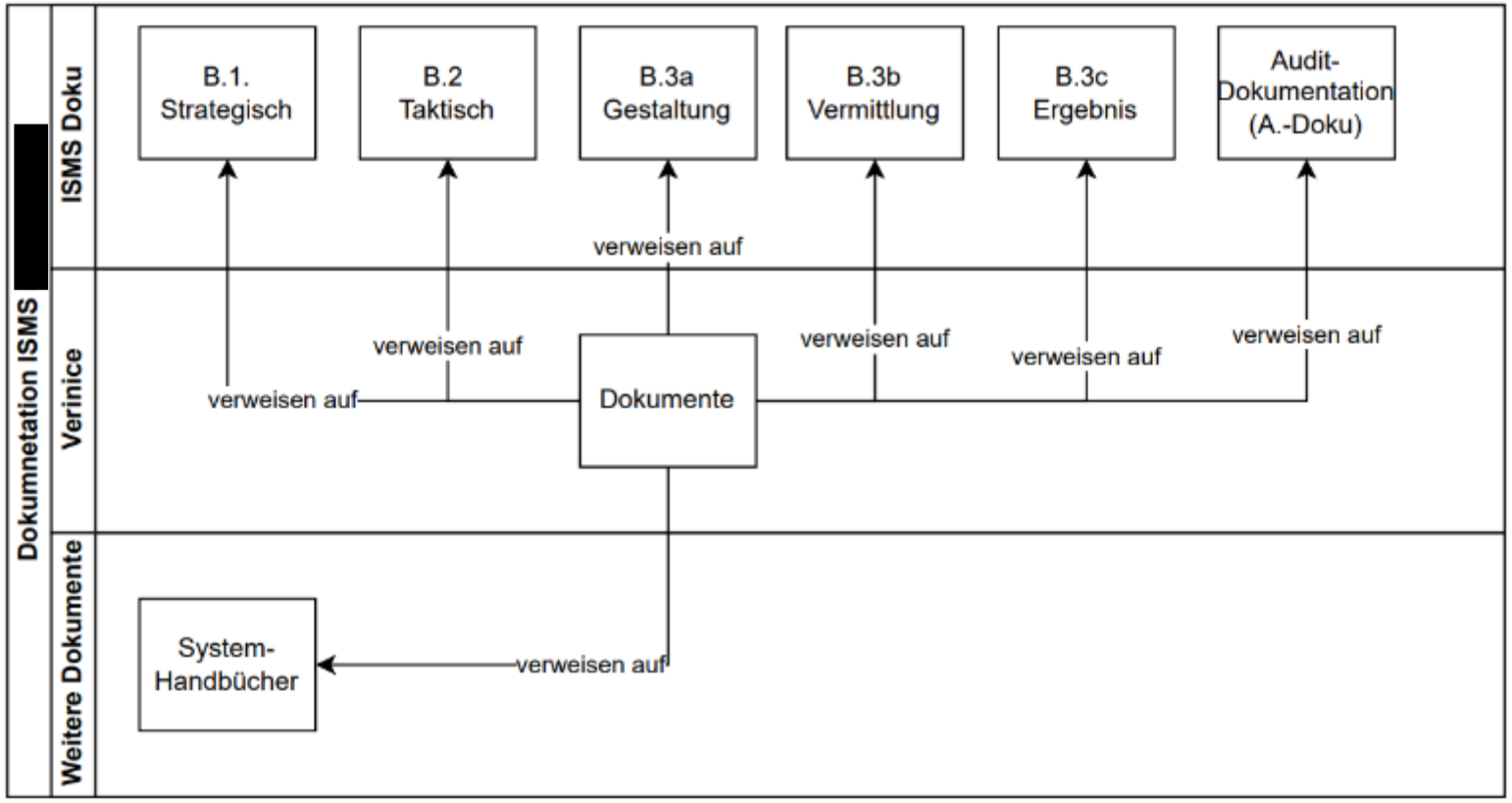
ISMS Dokumentation



Wird im vernice abgebildet



ISMS Dokumentation



Masterstandard

Einer sie zu (ver-)binden

- Festlegen mit welchem Standard Sie arbeiten wollen
- Feststellen ob es für die geforderten Anforderungen Mapping Tabellen zum Master gibt

- ToDos
  - Nutzen der Modernisierten GS Perspektive
  - Anlegen des Masters als Maßnahmen
  - Anlegen der anderen Standards als Bausteinanforderungen
  - Verknüpfen des Master mit den Anforderungen nach Mapping Tabelle.

Und was ist nu mit RUN

Master - KdA

- Alle Anforderungen als Maßnahmen erstellt
- Verknüpfunng mit Anforderungen lt. Mapping Tabelle RUN

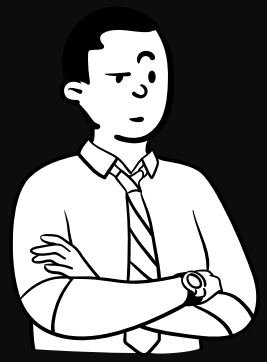
RUN Model Baustein Anforderungen

- Anlegen der Bausteine ISMS, BCMS
  - Anforderungen = Reifegrad
  - Bearbeitung „per Hand“
- Anlegen der Bausteine
  - Organisatorische Maßnahmen (OrgM)
  - Personenbezogene Maßnahmen (PerM)
  - Physische Maßnahmen (PhyM)
  - Technische Maßnahmen (TecM)
  - Umsetzungsgradbestimmung für die Detektion (SzA)
  - Anforderungen = Umsetzungsgrad
  - Bearbeitung durch Verknüpfung mit KdA als Maßnahmen
  - Umsetzung durch Maßnahmen ableiten

Projektende!

So nun mal im verinice

Noch Fragen?



iseco consulting

Vielen Dank für ihre Aufmerksamkeit!

Quellen:

- Reife- und Umsetzungsgradbewertung im Rahmen der Nachweisprüfung (RUN)
- Anforderungen nach § 8a Absatz 5 BSIG - Grundsätzliche Anforderungen im Nachweisverfahren (GAiN)
- Konkretisierung der Anforderungen an die gemäß § 8a Absatz 1 und Absatz 1a BSIG umzusetzenden Maßnahmen