SoftED SYSTEMS

IT-TRAINING · SOFTWARE · IT-CONSULTING

Grundschutz++
Reförmchen oder Umbruch?

verinice.xp 2026

Disclaimer

- Alle Angaben entsprechen dem öffentlich verfügbaren Informationsstand bis zum 10. Februar 2026.
- Meine persönliche Einordnung und Einschätzung, nicht vom BSI geprüft, freigegeben oder autorisiert.
- Sehen Sie diesen Vortag als Aufzeichnung, prüfen Sie ob inzwischen geänderte Informationen vorliegen.

Agenda

1) Ausgangslage
2) Was ist IT-Grundschutz++?
3) Was ändert sich grundlegend?
4) Was bleibt gleich?
5) Auswirkungen auf die Praxis
6) Einordnung und Handlungsempfehlungen

Ausgangslage

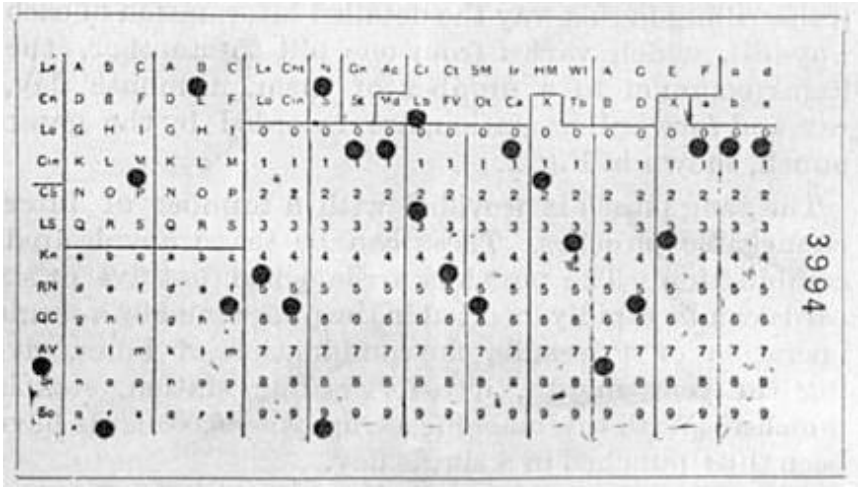
- Modernisierter IT-Grundschutz 2017-2025
  - Über 100 Bausteine, ca. 8000 Anforderungen, Redundanz als Prinzip
- Stand der Technik von 2022
  - Keine KI
  - Zero Trust/ Identity-First-Security nur als Rudiment
- Vermisste Themen/ Bausteine
  - KI-Security
  - Cloud-Native/ Kubernetes-Cluster

Grundschutz ++ Ausgangslage

- Kompendium im Oscal Format verfügbar
- Methodik und Begleitdokumente im Verlauf 2026
- Realistische Verwendung ab 2027 – Übergangsphase bis 2029?
- Umstieg verpflichtend (Bund, Länder, tw. weitere öffentliche Verwaltung)
- Einsatz möglich für nicht-staatliche Organisationen bspw. zur Erfüllung wesentlicher (nicht aller) NIS-2 Anforderungen

Was ist Grundschutz++?

- Format
  - » Statt doctype XML ->> OSCAL (JSON/XML)



Stand-der-Technik-Bibliothek / Quellkataloge / Methodik-Grundschutz++ / **BSI-Methodik-Grundschutz++-catalog.json**

MietherRaphael Update

Code | Blame | 7091 lines (7091 loc) · 370 KB


```
{
  "catalog": {
    "uuid": "2ac24b2e-7bfb-4ac5-8c7b-e0a6019d6187",
    "metadata": {
      "title": "BSI Methodik Grundschutz++",
      "published": "2026-02-05T15:31:33.928518+00:00",
      "last-modified": "2026-02-05T15:31:33.928518+00:00",
      "version": "1.0",
      "oscal-version": "1.1.2",
      "remarks": "Dieser Katalog enthält die Methodik-Grundschutz++, d.h. das Verfahren zum Aufbau eines ISMS nach Grundschutz++.",
      "roles": [
        {
          "id": "publisher",
          "title": "Publisher"
        }
      ],
      "parties": [
        {
          "uuid": "34da5f00-0c95-4196-b028-7b043ee29f3b",
          "type": "organization",
          "name": "BSI, Grundschutz++",
          "email-addresses": [
            "it-grundschutz@bsi.bund.de"
          ]
        }
```

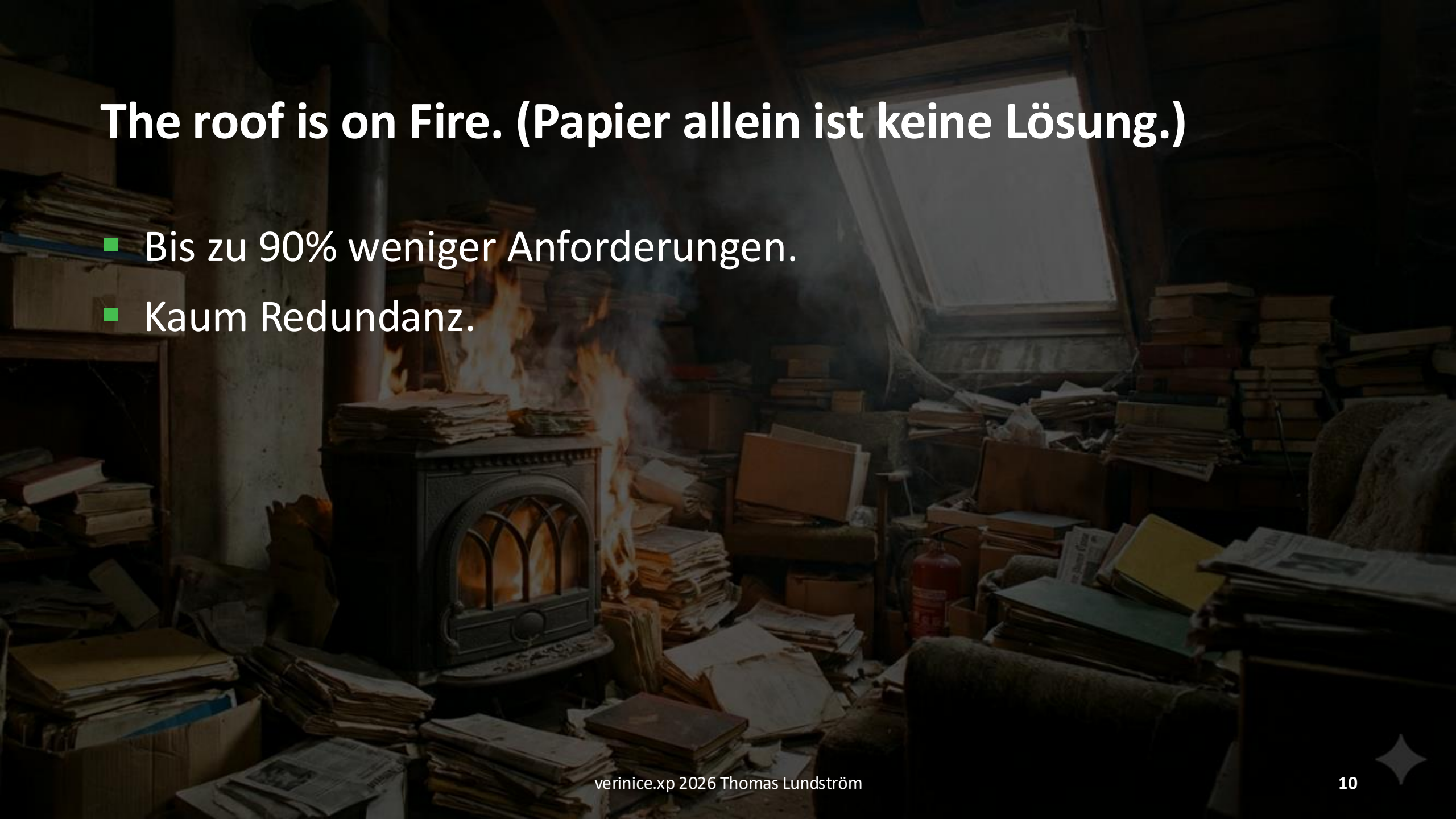
Veröffentlichungszyklen

- Mod. IT-Grundschutz
  - » Redaktionsschluss Oktober
  - » Veröffentlichung Februar
  - » (Letztmalig Feb. 2023)
- Grundschutz++
  - » Permanent auf github
  - » Codeberg wird aktuell nicht genutzt

Neue Features

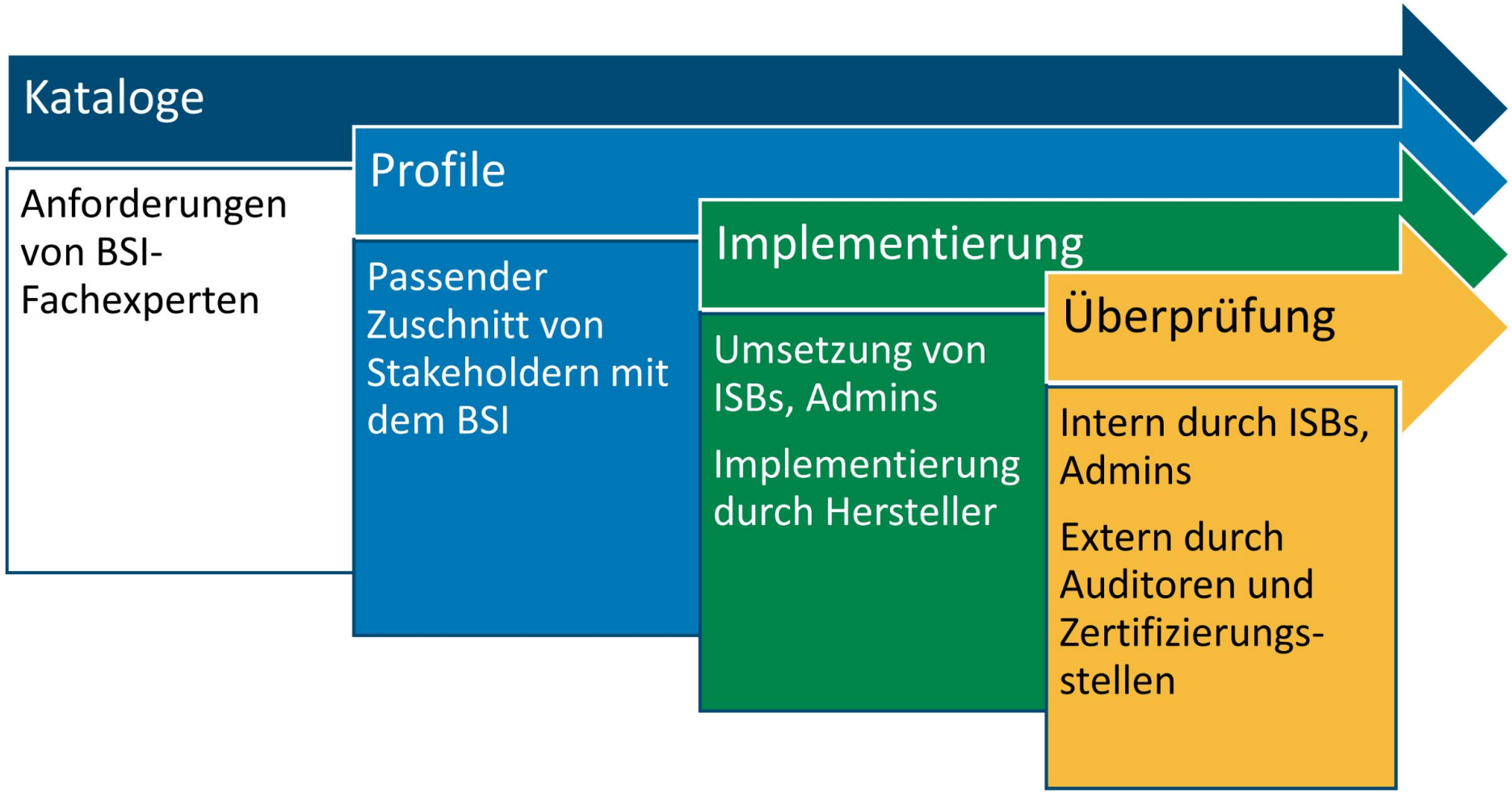
- Priorisierungsmodell in 6 Stufen statt Basis/ Kern / Standardvorgehen
- Blaupausen als neues Konzept
  » Definierte Assetgruppen mit Anforderungen

The roof is on Fire. (Papier allein ist keine Lösung.)



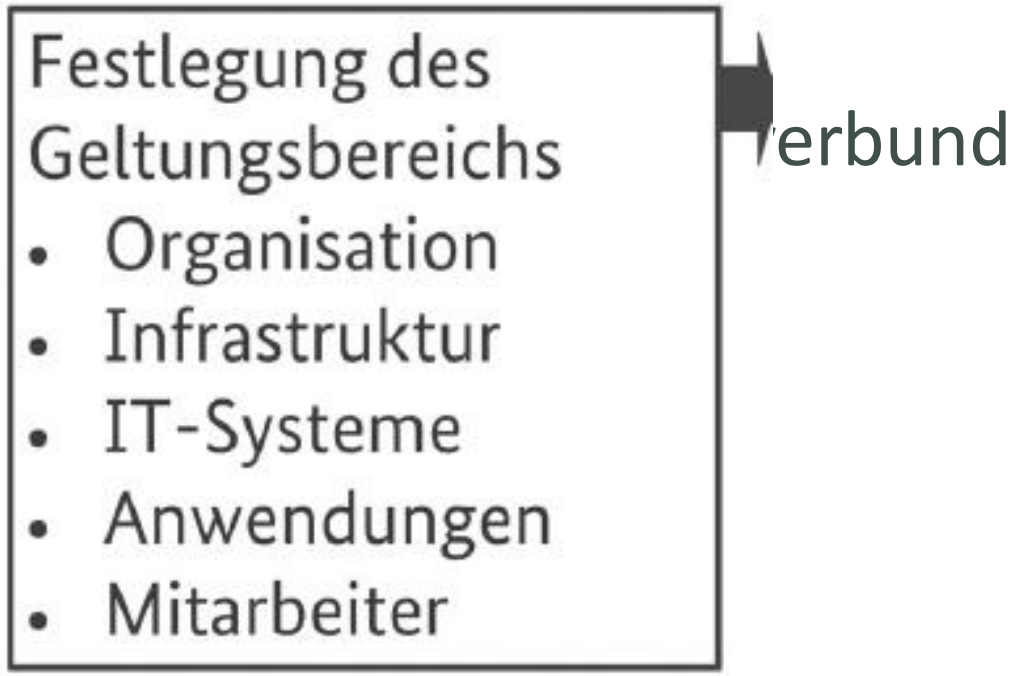
- Bis zu 90% weniger Anforderungen.
- Kaum Redundanz.

OSCAL ist mehr als eine Formatdefinition



SoftED SYSTEMS

Vergleich – Schritt für Schritt

- Modernisierter BSI IT-Grundschutz
- 

verbund

- OSCAL
  - » *System Security Plan* (SSP)
    - » System-Identifikatoren, System-Zweck, System-Kategorien, Betreiber, Standorte und vernetzte Dienste
  - » catalog / profile
    - » Auswahl von Maßnahmen (Controls)
    - » G++
    - » SDM 4.0?
    - » Company Compliance…

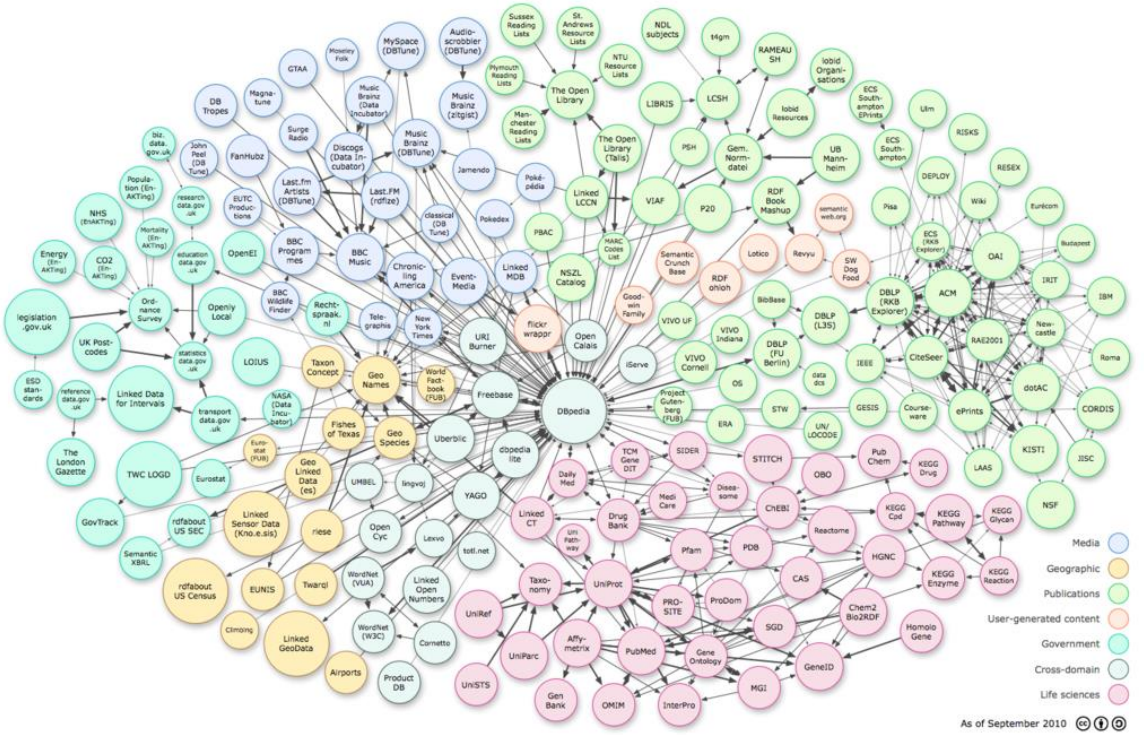
Strukturanalyse

- Mod. IT-Grundschutz
  - » Gruppieren
  - » Abhängigkeiten zwischen Zielobjekten erfassen

Geschäftsprozess	Anwendung								
	A001	A002	...	A009	A010	...	A013	A014	...
GP001 *Produktion*	X			X	X			X	
GP002 *Angebotswesen*	X	X		X	X		X		
GP003 *Auftragsabwicklung*	X	X		X	X		X		
GP004 *Einkauf*	X	X			X		X		
GP005 *Disposition*	X	X		X	X		X		

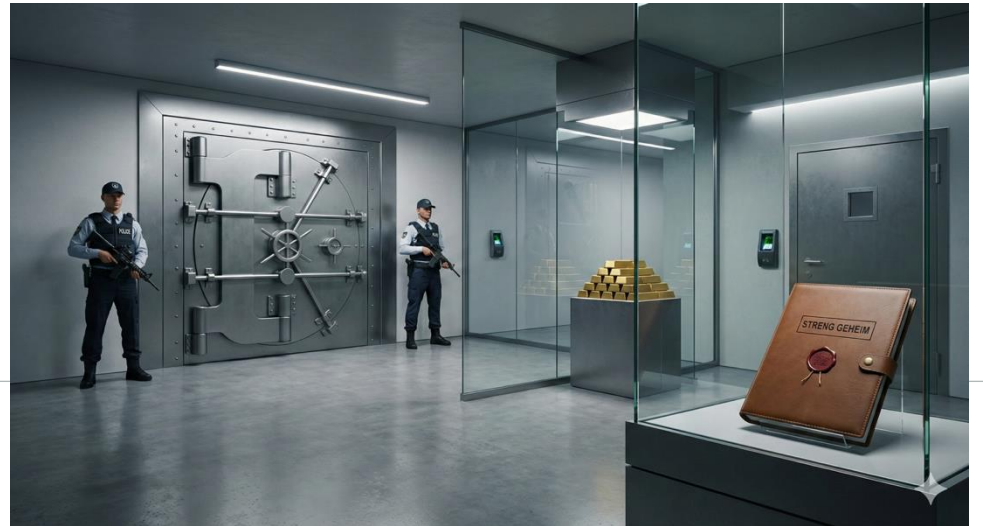
Tabelle 3: Zuordnung von Anwendungen zu Geschäftsprozessen

- OSCAL
  - » UUID im prop/link-Attribut als description



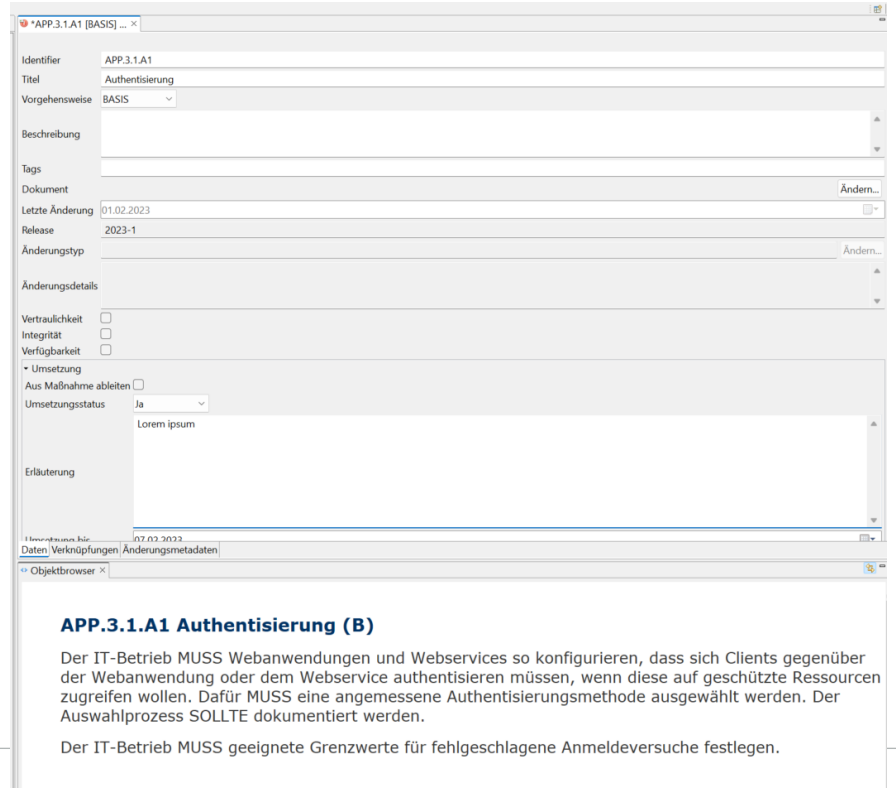
Schutzbedarfsfeststellung und Vererbung

- Mod. IT-Grundschutz
  - » Prozess gibt SB vor
  - » Anwendungen erben von Prozessen
    - » Clients von Anwendungen
    - » Server von Clients
    - » Netze von Clients und Servern
    - » Räume von Netzen
- Grundschutz++
  - » OSCAL kann SB für Scope erfassen
  - » OSCAL kann für Assets „security-level“ in eigenen props erfassen
  - » ISO 27001:2022 zwingt zu Klassifikation nach Wert, Sensitivität und Kritikalität (CIA)



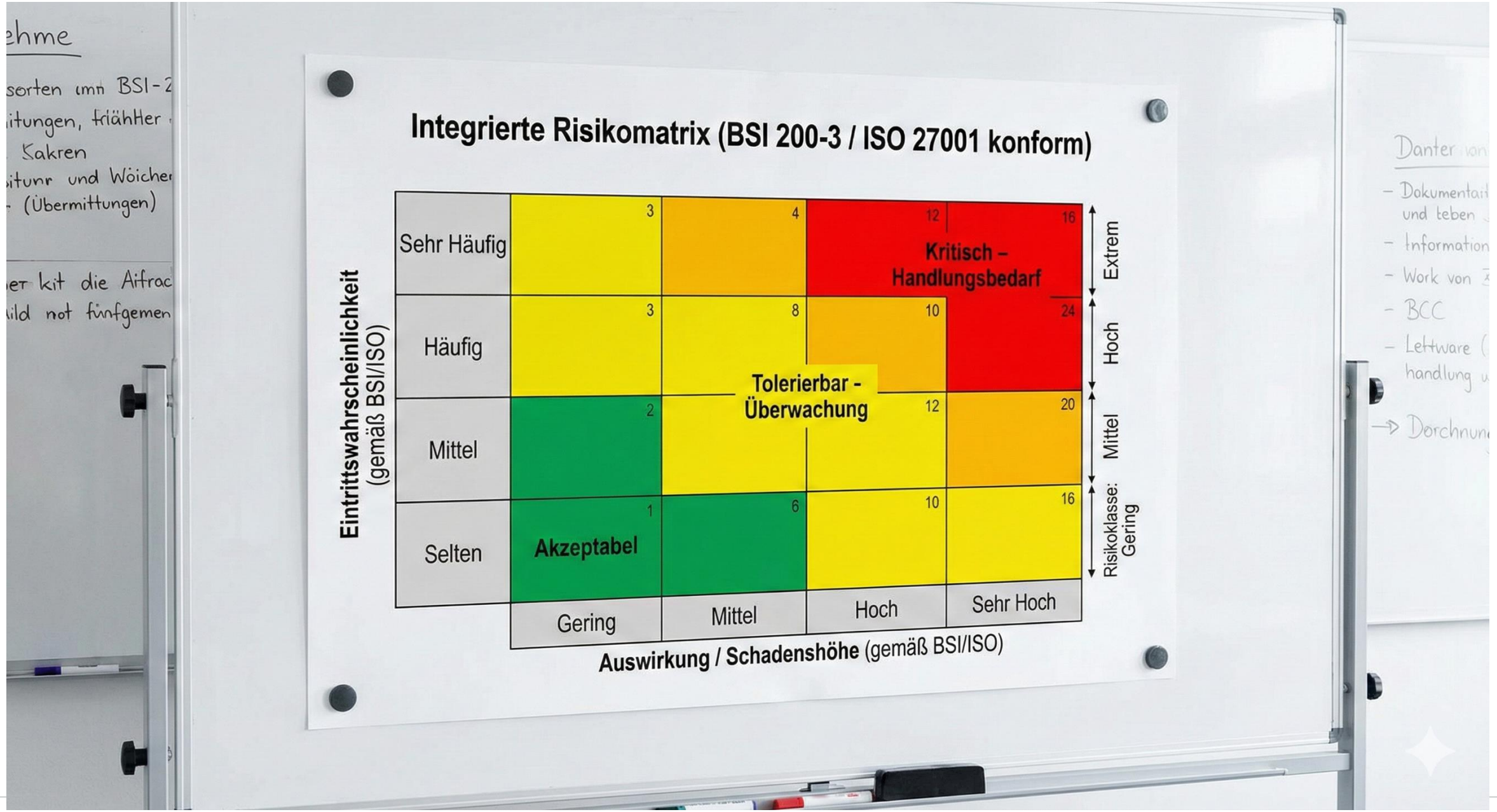
Check

- Mod. IT-Grundschutz
  - » Ja, Nein, Teilweise
  - » Entbehrlich



- Grundschutz++
  - » oscal kann per Asset implementation-status (mit Werten wie implemented, partially-implemented, planned, not-applicable)

SoftED SYSTEMS



Implizite Risikoanalyse

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein APP.6 *Allgemeine Software* von besonderer Bedeutung.

2.1. Ungeeignete Auswahl von Software

Für viele Anwendungszwecke und Einsatzmöglichkeiten werden die unterschiedlichsten Software-Lösungen auf dem Markt angeboten. Wird eine unpassende Software, die nicht den Anforderungen der Institution entspricht, ausgewählt, dann kann der Betrieb erheblich gestört werden. Dateiformate könnten zum Beispiel nicht mit bereits eingesetzten Programmen kompatibel sein oder neue Produkte einen zu geringen Funktionsumfang haben. Das kann zu Leistungsverlusten, Störungen oder Fehlern innerhalb der Geschäftsprozesse führen.

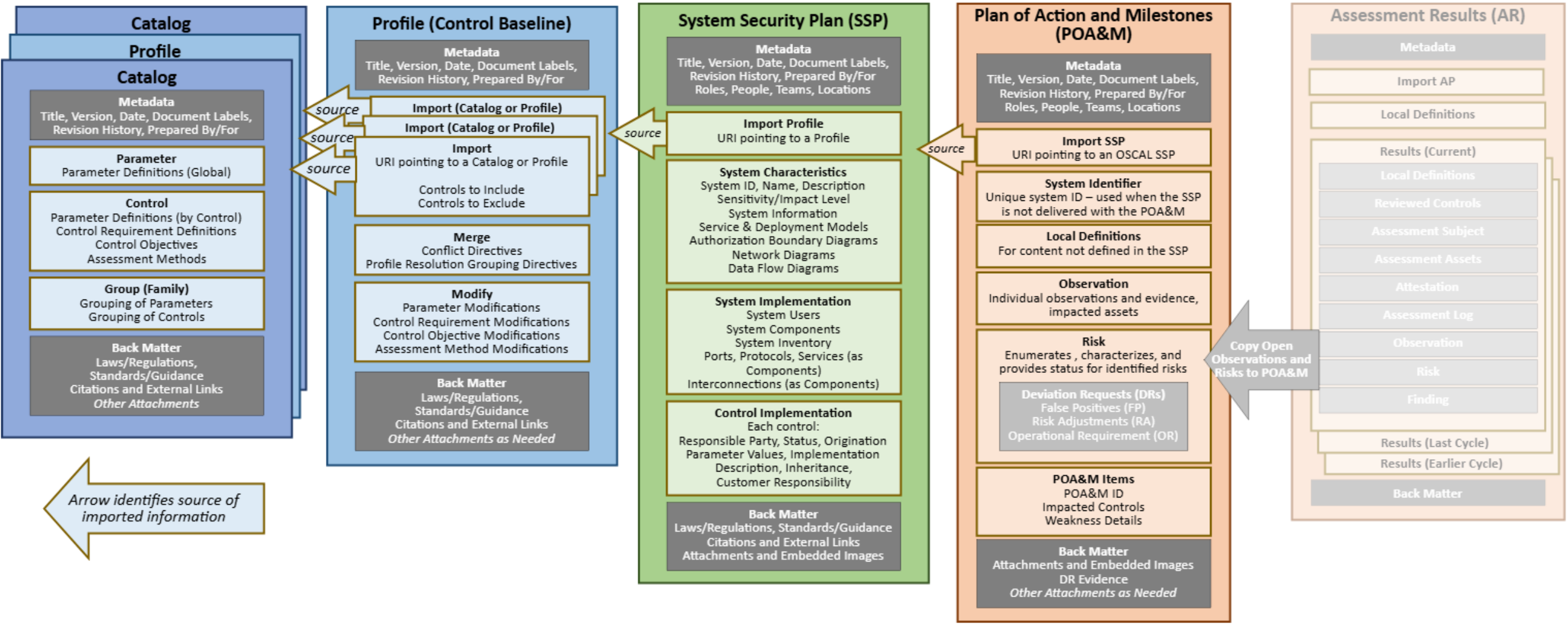
Insbesondere wenn die Software nicht die Sicherheitsanforderungen der Institution erfüllt, könnten die mit der Software verarbeiteten Daten offengelegt oder manipuliert werden, z. B. wenn Login-Funktionen von Anwendungen nicht für die geplante Einsatzumgebung in einem offenen Datennetz konzeptioniert worden sind.

2.2. Offenlegung schützenswerter Informationen durch fehlerhafte Konfiguration

Ist eine Software fehlerhaft konfiguriert, können unbeabsichtigt schützenswerte Informationen offengelegt werden, z. B. wenn nicht benötigte Funktionen noch aktiviert sind, wie Cloud-Backup-Funktionen, die Daten ungewollt in eine Cloud synchronisieren. Hierdurch könnten sensible Daten von unbefugten Dritten eingesehen und offengelegt werden.

Das kann zu finanziellen Einbußen führen oder die Reputation einer Institution schädigen. Zusätzlich könnte die Institution auch gegen geltendes Recht verstoßen, z. B. wenn personenbezogene Daten offengelegt werden.

- Ablage in oscal möglich (PoA&M Plan of Action & Milestones)
- Mapping zu Anforderungen (oscal sprech „Maßnahmen“) möglich
- Dringend gewünschte Arbeitserleichterung.



SOFTED SYSTEMS

Umsetzungsplanung/ Risikoakzeptanzbericht

- Mod. IT-Grundschutz
  - » GS-Check Delta
  - » + GS Standard Anforderungen die „Entbehrlich“ gekennzeichnet wurden
  - » +zusätzliche Sicherheitsmaßnahmen aus den Ergebnissen der Risikoanalyse

- Grundschutz++
  - » oscal erfasst per Asset und Anforderung Status der Umsetzung (implemented, planned, partially-implemented etc.) in implemented-requirements und implementation-status
  - » Verweise auf Meilensteine, Fristen oder Projekte können als remarks, props oder links ergänzt werden

```
SSP → control-implementation:
 ├── implemented-requirement:
|    ├── status: "planned"
|    ├── remarks: "Umsetzung Q2/2026 durch Projekt XYZ"
|    └── responsible-role: "CISO"

POA&M → poam-item:
 ├── risk: "Offene Authentifizierungslücken"
 ├── action: "Multi-Factor einführen"
 ├── milestone: {due-date: "2026-06-30"}
 └── status: "in-progress"
```

Chance 1: Neue Automatisierungsmöglichkeiten

- Integration in Tools ohne manuellen Eingriff
- Prüfung maschinenprüfbarer Anforderungen automatisiert (Bspw. GPOs, FW Rulesets, Kryptografiemethoden….)
- KI unterstützte Dokumentationsaudits

Chance 2 – Flexibilität und Agilität

- Dynamische Anpassung an neue Bedrohungen
- Modulare Praktiken statt starrer Bausteine
- Branchenspezifische Blaupausen verfügbar*
- Schnellere Reaktion auf technologische Entwicklungen

Chance 3 – Effizienzgewinn

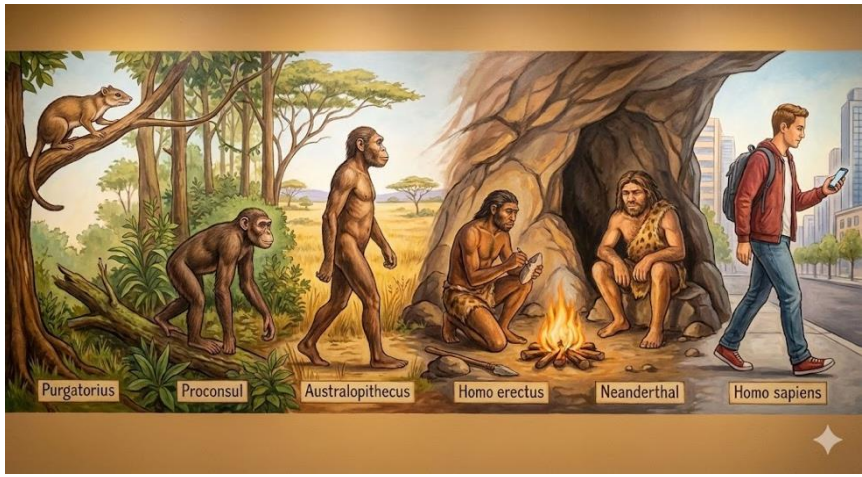
- Reduzierung der MUSS-Anforderungen auf unter 10%
- Weniger Redundanzen durch intelligente Modularisierung
- Schnellerer Einstieg durch Quick-Win-Maßnahmen (Stufe 0/1)
- Gezielte Budgetentscheidungen durch transparente Priorisierung

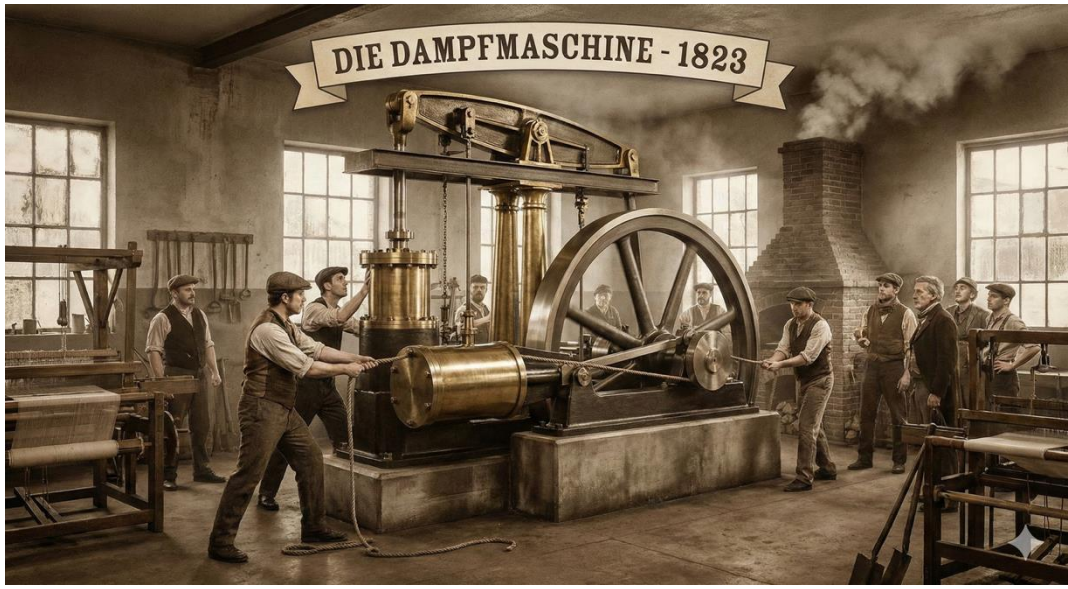
03:17 AM
Mitre ATT&CK Matrix
CRITICAL
CRITICAL
Cyber Kill Chain
CVE-2026-1234
CVE-2025-5678
Reconnaissance
Weaponization
Delivery
Exploitation
Installation
C2
Actions on Objectives


03:17 AM
Riditiak
5
12
13
24
25
4
11
18
19
20
3
6
12
15
18
9
7
8
2
1
Riditisk
25 - Katastrophal
Szenario: Datenverlust durch Ransomware (KRITISCH)
Gyber Kill Chain
Seccnelesence
Noagnatation
Delivery
Explsitetion
Inctallation
02
Actions en Objectives

Evolution oder Revolution/ Disruption?

- Methodik grundlegend verändert aber
- ISO 27001:2022 bleibt Richtschnur
- Konkrete Umsetzung und Beschreibungstiefe entscheidet
- Echte Chance auf ISO ++ oder grundlegende Überarbeitung 2030.





SoftED SYSTEMS

Vielen Dank für Ihre Aufmerksamkeit!

SoftED SYSTEMS