# Grundschutz++ trifft Kommune

## Das koBA-Profil zwischen IT-Grundschutz und Grundschutz++



Kassel

# Das koBA-Profil — was wir gebaut haben

IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung (koBA-Profil)

ZIELBILD

## Ein realistischer, praktikabler Einstieg in den Grundschutz für Kommunen — mit einem klar definierten kommunalen Mindestsicherheitsniveau.

*Wir haben nicht den großen Wurf entwickelt, sondern die kleine Hürde gesenkt — damit Sicherheitsarbeit in Kommunen überhaupt anfängt.*

### Zielbild

Mindestsicherheitsniveau für Kommunalverwaltungen

### Referenzinfrastruktur

Typische kommunale Objekte, Netze, Systeme, Räume

### Anforderungsauswahl

Basis-Anforderungen + kuratierte Standard-Anforderungen

### Kommunale Hinweise

Abweichungen, Priorisierung, Umsetzung in der Praxis

**503**
Anforderungen im Profil

**75**
relevante Bausteine

**≈ 95 %**
Basis-Anforderungen abgedeckt



Kassel

# Drei Zahlen aus dem koBA

Wer das versteht, versteht das Profil

**75 / 112**

Bausteine

### Strukturmodellierung

Nur die für eine „1. Verteidigungslinie“ tatsächlich relevanten Bausteine. Für eine vollständige Basis-Absicherung wären zusätzlich mindestens fünf weitere Bausteine umzusetzen.

Das ist keine Anforderungsfilterung, sondern Modellierung.

**368 / 368**

Basis-Anforderungen

### Vollständig übernommen

Innerhalb der 75 einbezogenen Bausteine wurden die Basis-Anforderungen übernommen.

**+ 130**

Standard-Anforderungen

### Gezielte Anreicherung

Sorgfältig kuratiert nach Bewertungsmatrix: Breitenwirkung, Risikoreduktion, Quick-Win, kommunale Mindestnotwendigkeit. Hinzu kommen 5 Hoch-Anforderungen.



Kassel

# Was der Grundschutz++ mitbringt — und was nicht

Anschluss an den BSI-Vortrag

## Was es gibt

- **998 Anforderungen**
  im neuen Anwenderkatalog, OSCAL-basiert
- **Zwei Sicherheitsniveaus**
  normal-SdT (772) und erhöht (226)
- **Aufwand 0 bis 5**
  als Umsetzungs-Indikator
- **MUSS · SOLLTE · KANN**
  klare Modalverben statt Stufentexte
- **19 Praktiken**
  Methodik · technisch · organisatorisch
- **41 Zielobjektkategorien**
  Strukturmodellierung über Assets

## Was es nicht mehr gibt

- **Basis-Stufe entfällt**
  Begriff existiert im GS++ nicht mehr
- **Bausteine entfallen**
  Stattdessen Praktiken, Anforderungen und Zielobjekte
- **ID-Mapping fehlt**
  ISMS.1.A1 hat im GS++ keine Entsprechung
- **Profil-Begriff verändert**
  IT-Grundschutz-Profile heißen Blaupausen, sind aber keine
- **Mindestniveau unter normal-SdT entfällt**
  Nur über Risikobetrachtung dokumentierbar
- **Referenzarchitektur-Format fehlt**
  Methodik beschreibt (noch) keine Implementierung als Sicherheitskonzept



Kassel

# Das Kernproblem in einem Satz

Basis war nie eine Filterfunktion

**„Basis“** ist eine ***Wirkungsklasse*** — kein Schutzbedarfsniveau und kein Aufwandsmaß.

### 1 normal-SdT ist das volle Niveau

Es bezeichnet den heute geltenden Stand der Technik bei normalem Schutzbedarf — nicht eine Einstiegsschwelle darunter.

### 2 MUSS ist nicht inhaltlich Basis

Im Anwenderkatalog gibt es 152 MUSS-Anforderungen — überwiegend identische Methodik-Pflichten je Praktik. Keine technische Schutzmaßnahme.

### 3 Aufwand bewertet Umsetzung

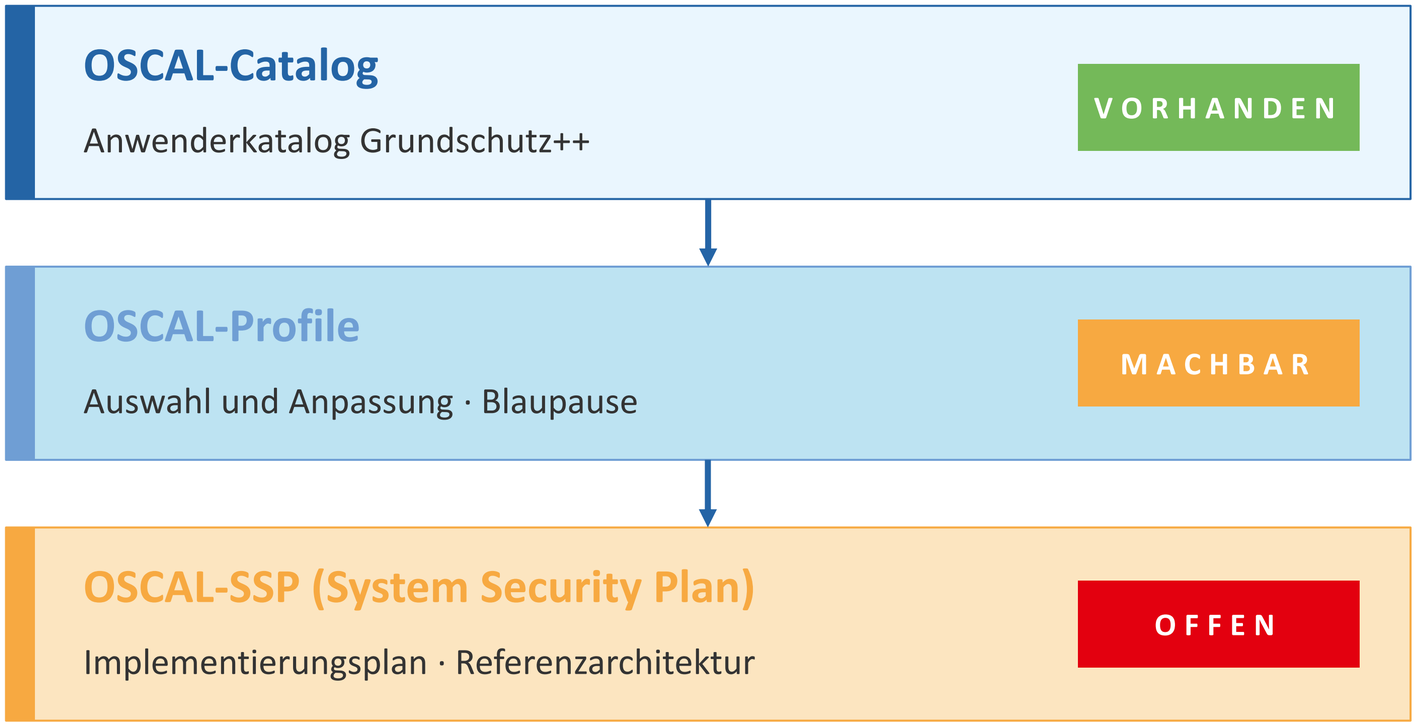
Eine Firewall einzurichten ist Basis und Aufwand 4. Eine Konzeptpflicht kann Aufwand 1 sein und gehört trotzdem nicht zu Basis.



Kassel

# Die OSCAL-Ebenen — wo das koBA wirklich liegt

Ein Profil ist nicht nur eine Anforderungsliste




Was es zu wissen gibt: 998 Anforderungen, gepflegt vom BSI. Dieses Stück haben wir.

Welche Anforderungen für eine typische Kommune relevant sind — Auswahl, Parameter, Modalverb-Anpassung. Mit der Blaupausen-Suite machbar.

Wie eine kommunale Infrastruktur aussieht: Zielobjekte, Verantwortlichkeiten, Outsourcing-Konstellationen. Hier endet die heutige GS++-Methodik.

***Das bestehende koBA-Profil wäre im OSCAL-Framework Profile + SSP in einem Artefakt. Im GS++ gibt es dafür noch keine Bezeichnung.***



Kassel

# Wie es weitergehen kann

Vier Optionen, von einfach bis vollständig

## A

### Nur filtern

Kandidatenmenge aus normal-SdT + Aufwand ≤ 2. Schnell, aber fachlich nicht belastbar.

BEWERTUNG

**nicht empfohlen**

## B

### Reine Blaupause

OSCAL-Profile mit kuratierter Auswahl. Liefert das Anforderungspaket — ohne Referenzarchitektur.

BEWERTUNG

**übergangsfähig**

## C

### Blaupause + Referenz-SSP

Auswahl plus typische kommunale Infrastruktur als wiederverwendbares Artefakt (Muster-IT-Sicherheitskonzept). Derzeit Methodik-Lücke.

BEWERTUNG

**fachlich beste**

## D

### GS++ und koBA-Katalog

Option C zusätzlich mit kommunalspezifischen Anforderungen, die im GS++ fehlen, in einem eigenen Katalog. Pflegeintensiv.

BEWERTUNG

**saubere Zielarchitektur**



Kassel

# Offene Punkte

Worüber wir mit dem BSI sprechen müssen

01

## Methodische Lücke SSP

Die GS++-Methodik beschreibt fünf Prozessschritte, aber keinen veröffentlichungsfähigen System Security Plan als Artefakt. Wie kommt die kommunale Referenzarchitektur in OSCAL?

02

## Anerkennung kommunaler Blaupausen

Wer prüft eine kommunale Blaupause, wer registriert sie, wie wird sie über Jahre konsistent zum Hauptkatalog gepflegt? Heute gibt es keinen offiziellen Prozess.

03

## Niveau unter normal-SdT

Im alten Profil war Basis explizit unterhalb der Standard-Absicherung möglich. Im GS++ geht das nur mit dokumentierter Risikobetrachtung pro Anforderung. Gilt das für jede Kommune einzeln?

04

## Mapping alt zu neu

503 koBA-Anforderungen müssen einzeln auf den GS++-Katalog abgebildet werden. Eine Übersetzung ohne ein BSI-Mapping IT-Grundschutz → GS++ ist für Kommunen nicht leistbar.

05

## Begründungsprofile

Die Bewertungsmatrix der koBA hat sechs Kriterien. Im GS++ gibt es bisher kein Feld, um diese Begründung anforderungsweise mitzuführen. Erweitert sich der Katalog?

06

## Übergangszeit bis 2031

Die Zertifizierbarkeit nach IT-Grundschutz endet im Oktober 2031. Bis dahin müssen Kommunen den Übergang planbar gestalten können — Hilfsmittel, Schulungen, Migrationspfade.



Kassel

# Unser Vorschlag

Was die AG koBA jetzt anbietet

## VORAUSSETZUNG

### BSI-Mapping als Grundlage

- Bestehende Sicherheitskonzepte können nicht alle in GS++ neu erstellt werden
- Die GS++-Community fordert ein BSI-Mapping IT-Grundschutz → GS++
- Auf dieser Grundlage: spezifisches Mapping des koBA-Profils durch die AG
- Ohne BSI-Mapping kein tragfähiger Migrationspfad für Kommunen

## BLAUPAUSE

### Kommunale GS++-Blaupause

- Vorauswahl relevanter Praktiken und Zielobjektkategorien
- Anforderungen mit kommunalem Mindest-Tag versehen
- Begründungsprofile aus der koBA-Bewertungsmatrix
- Evaluierung nach einer Pilotierung mit drei bis fünf Kommunen verschiedener Größe

## REFERENZ-SSP

### Muster-Kommune in OSCAL

- Typische kommunale Infrastruktur als SSP-Vorlage
- Rathaus · Außenstelle(n)
- Outsourcing-Konstellationen mit kommunalen IT-Dienstleistern
- Abstimmung mit BSI über das Veröffentlichungsformat



Kassel

# Lassen Sie uns reden.

**Das koBA-Profil hat funktioniert, weil Kommunen es gemeinsam entwickelt haben.**
**Damit der Übergang in den Grundschutz++ wieder funktioniert, brauchen wir Sie.**

**Frage 1**

Welche kommunalen Lücken sehen Sie heute schon?

**Frage 2**

Welche Bestandteile braucht Ihre Kommune zwingend?

**Frage 3**

Wer macht bei der Migrationsarbeit mit?



Kassel