IT-Grundschutz zu Grundschutz++

Know-how to go

HiSolutions AG

Sebastian Reinhardt

Agenda

1. Ausgangslage
2. Ziele
3. Aktueller Stand/Sneak Peak
4. Fazit

Sebastian Reinhardt

Senior Expert IT-Grundschutz

Fachliche Schwerpunkte

- Aufbau und Betrieb von ISMS nach IT-Grundschutz und ISO/IEC 27001
- IT-Notfallmanagement
- Informationssicherheitskonzepte und -richtlinien
- Audits und Prüfungen
- Sicherheitsschulung und -trainings

Qualifikationen

- Zertifizierter IT-Grundschutz Praktiker
- Zertifizierter IT-Grundschutz Berater
- Zusätzliche Prüfverfahrenskompetenz gemäß § 8a BSIG
- Zertifizierter Lead Auditor ISO 27001
- Zertifizierter PRINCE2® Practitioner
- Information Security Officer (TÜV)
- Chief Information Security Officer (TÜV)

Ausgangslage

Erfolge des IT-Grundschutz

152 Zertifizierte Institutionen[1]

54 Laufende Verfahren[2]

Stand 08.02.2026

De-Facto-Standard in DE (Öffentliche Verwaltung)

Internationale Vorlage für weitere Standards (ISKE-Estland)[3]

Nutzung im Rahmen von KRITIS & häufige Referenz für ISO 27001

Ausgangslage

Strukturelle Herausforderungen bei der Umsetzung

Bund: Stagnation trotz Pflicht

- Verpflichtung seit 2017
- Umsetzungsstand 2025 „erschütternd“[4]

Länder: Heterogener Reifegrad

- Eigenständige IS-Gesetze
- „Angemessenheit“ gefordert
- Häufig jedoch noch Lückenhaft

Kommunale Ebene: Bewusstsein vs. Realität[5]

57 %

der Kommunen sehen Cyber-Angriffe als ernsthafte Bedrohung

35 %

der Kommunen verfügen über ein aktuelles Sicherheitskonzept

Ziele

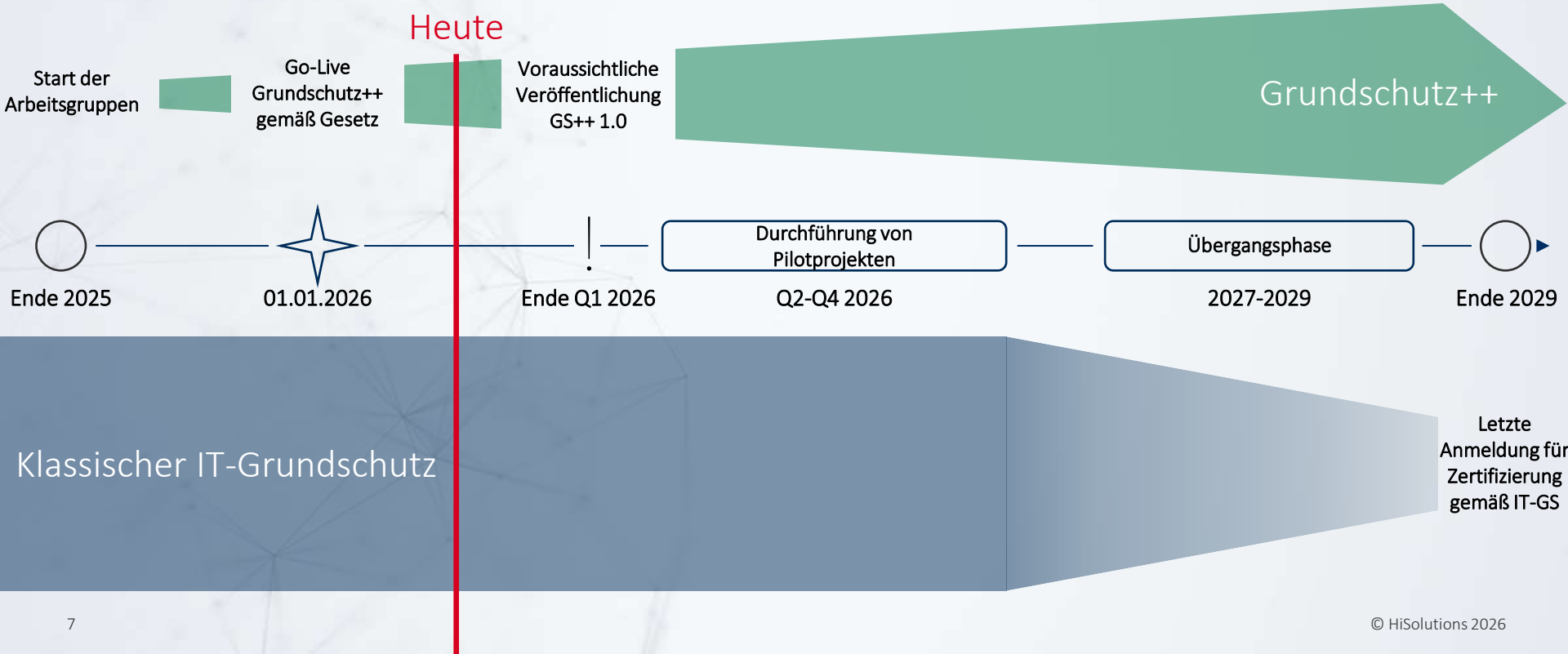
Transformation des IT-Grundschutz

- Radikale Entbürokratisierung
- Automatisierung & Maschinenlesbarkeit
- Neue Struktur
- Messbarkeit & KPIs

Transformation gemäß NIS-2-Umsetzungsgesetz bis 01.01.2026

Aktueller Stand

Zeitplan der Transformation



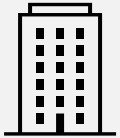
Aktueller Stand

Zielgruppe und Anwendungsbereiche laut BSI*

Kleine Institutionen

Schlanker Einstieg für begrenzte personelle und zeitliche Ressourcen

Mittlere Institutionen



Skalierbarkeit von Prozessen und Teilautomatisierbarkeit

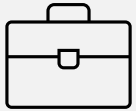
Große Institutionen

Integration in komplexe Landschaften & **weitreichende Automatisierung**smöglichkeiten

Einsatz von IT-Grundschutz/GS++

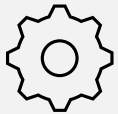
Bundesverwaltung (BSIG § 44):
Verbindlich ab 01.01.2026

Wirtschaft (NIS-2):
Referenzstandard



Entscheidungsebene:
Ressourcen & Initiierung

Sicherheitsmanagement:
Steuerung (ISB/CISO)



Operative Ebene:
Umsetzung & Betrieb

*Diese und alle folgenden Angaben basieren auf dem letzten Diskussionspapier und sind vorbehaltlich jeglicher Änderungen durch das BSI

Aktueller Stand

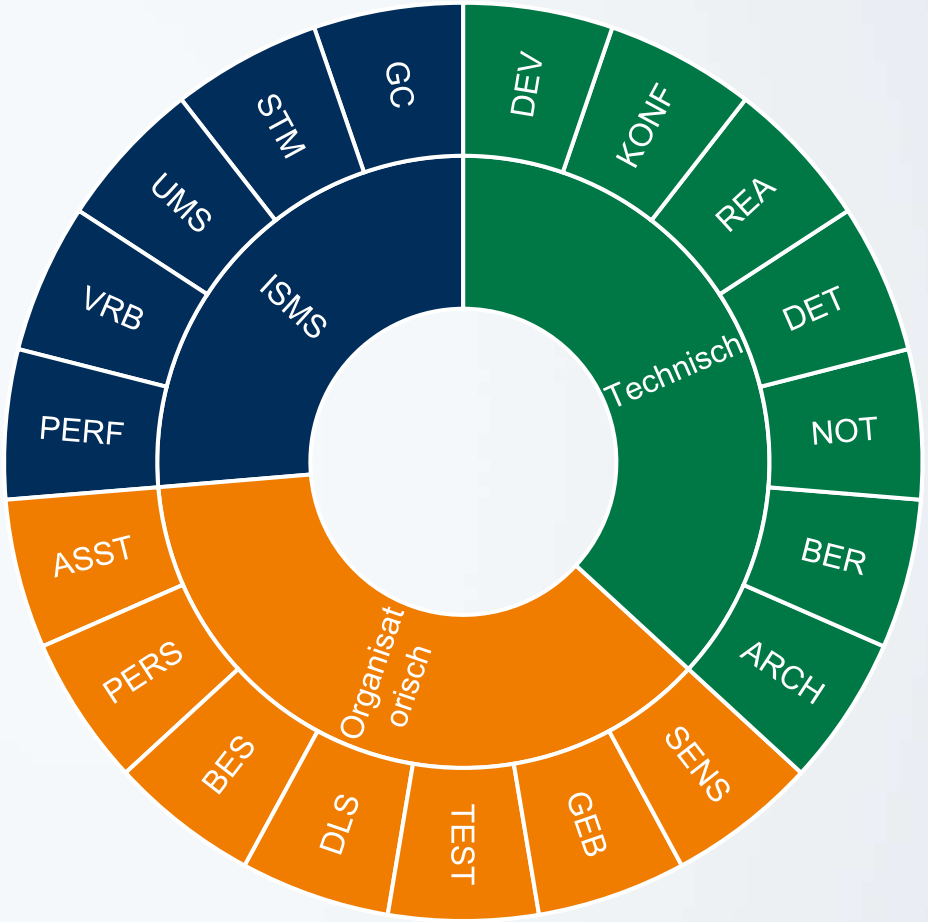
Die 19 Praktiken

Praktik != Baustein

Bündelung von Anforderungen an bestimmte Prozesse innerhalb einer Organisation mit konkreten Auswirkungen auf Rollen, Abläufe oder Assets.

Unterscheidung von drei Praktik-Kategorien:

- ISMS
- Organisatorisch
- Technisch



Aktueller Stand

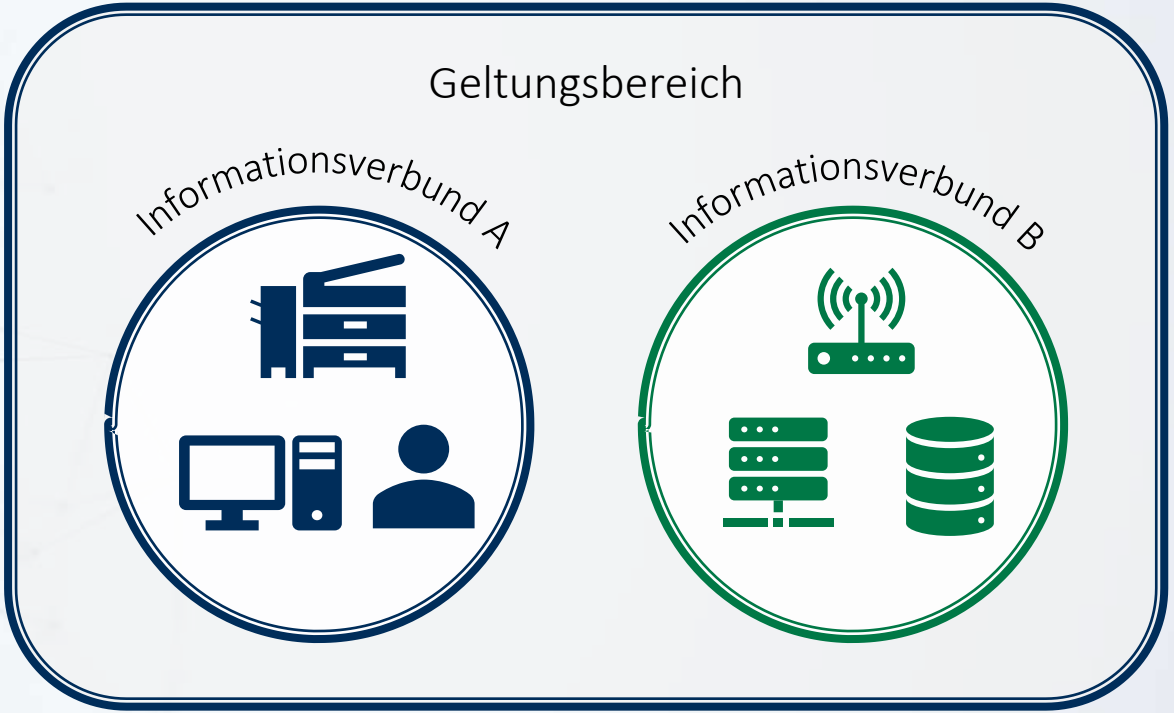
Geltungsbereich/Informationsverbund

Geltungsbereich

Definiert den formalen und organisatorischen Umfang des ISMS. Grenzt ab, welche Bereiche, Standorte und Prozesse geschützt werden.

Informationsverbund

Die technische/inhaltliche Abbildung des Geltungsbereichs. Hier entsteht das konkrete Sicherheitskonzept.



Aktueller Stand

Prozesszyklus

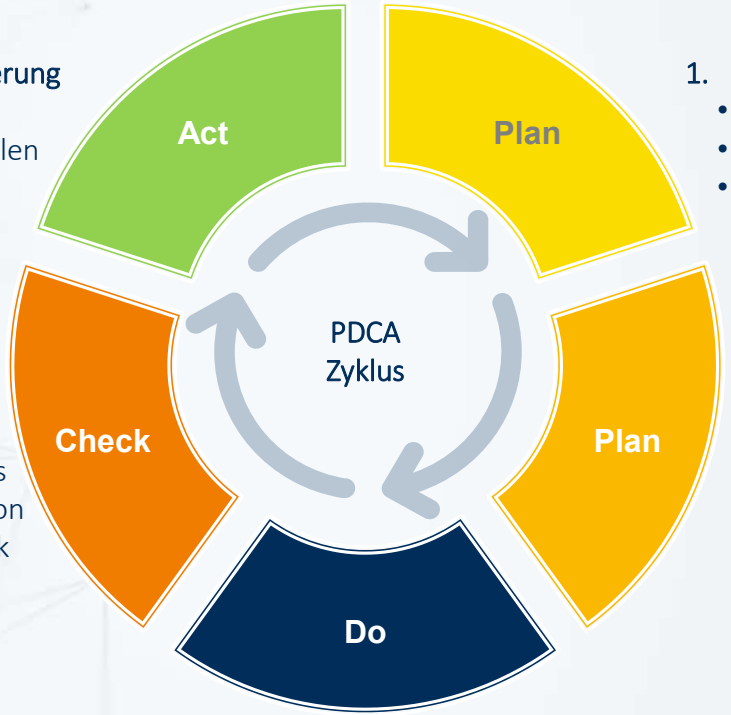
1. **Erhebung & Planung**
   - Governance & Compliance
   - Kontext & Leitlinie
   - Organisation & Rollen

2. **Anforderungsanalyse**
   - Strukturmodellierung
   - Schutzbedarf & Risiken
   - Anforderungskatalog

3. **Realisierung**
   - Umsetzung & Betrieb
   - Soll-Ist-Vergleich
   - Sensibilisierung

4. **Überwachung**
   - Monitoring & KPIs
   - Audits & Evaluation
   - Compliance Check

5. **Kontinuierliche Verbesserung**
   - Korrekturmaßnahmen
   - Behandlung von Vorfällen
   - Optimierung des ISMS



Aktueller Stand

Prozessschritt 1: Erhebung und Planung

Strategische Verankerung & Governance

- „Warum“ & „Wer“ ?
- Ausrichtung an Institutionszielen
- Explizite Leitungs-verantwortung
- Verabschiedung der Sicherheitsleitlinie

Kontext, Scope & Kritikalität

- „Wo“ & „Was“ ?
- Umfeldanalyse
- Definition des Geltungsbereichs
- Identifikation „kritischer“ Geschäftsprozesse

Organisation, Compliance & Risiko

- „Wie“ ?
- Compliance Management
- Etablierung unabhängiger Rollen (z. B. ISB)
- Risikomanagement

Fazit:
Das Fundament für das ISMS ist gelegt. Der organisatorische und strategische Rahmen ist gesetzt, und die Institution kennt die kritischen Werte. Risiken werden aktiv verwaltet, und die notwendigen Strukturen für eine operative Umsetzung von Anforderungen sind vorhanden.

Aktueller Stand

Prozessschritt 2: Anforderungsanalyse

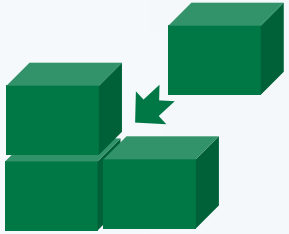
1. Priorisierung & Auswahl

Identifikation kritischer Prozesse (Fokus auf Geschäftszweck)

2. Erfassung & Zerlegung

Erfassung von Assets und Zerlegung in entsprechende Kategorien (Informationen, Anwendungen, IT-Systeme, etc.)

3. Modellierung



Mapping der Assets auf „**Zielobjektkategorien**“ innerhalb von relevanten Praktiken

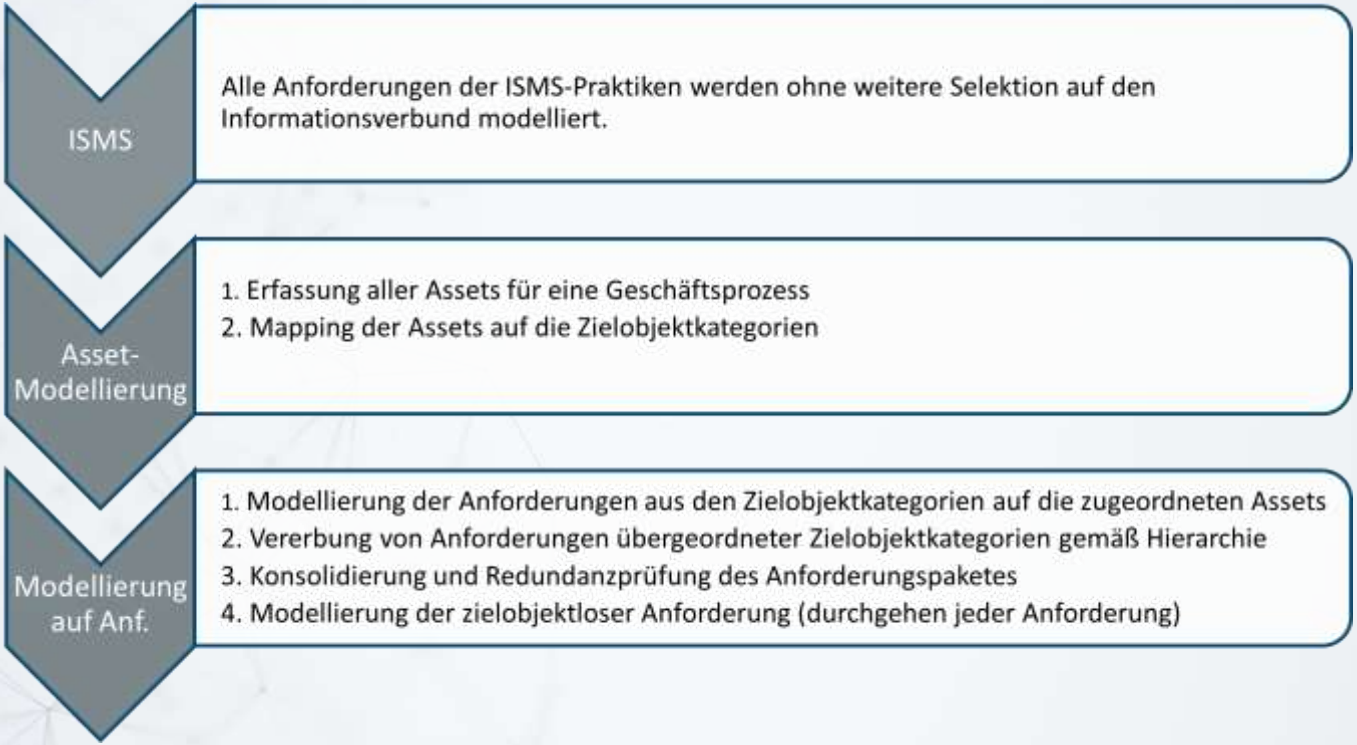
4. Anforderungspaket

Individuelle Liste aller umzusetzenden Anforderungen

Für Prozesse mit einem „hohen“ Schutzbedarf ist eine gesonderte Risikobetrachtung notwendig, um ggf. risikoorientiert weitere individuelle Anforderungen zu erarbeiten

Aktueller Stand

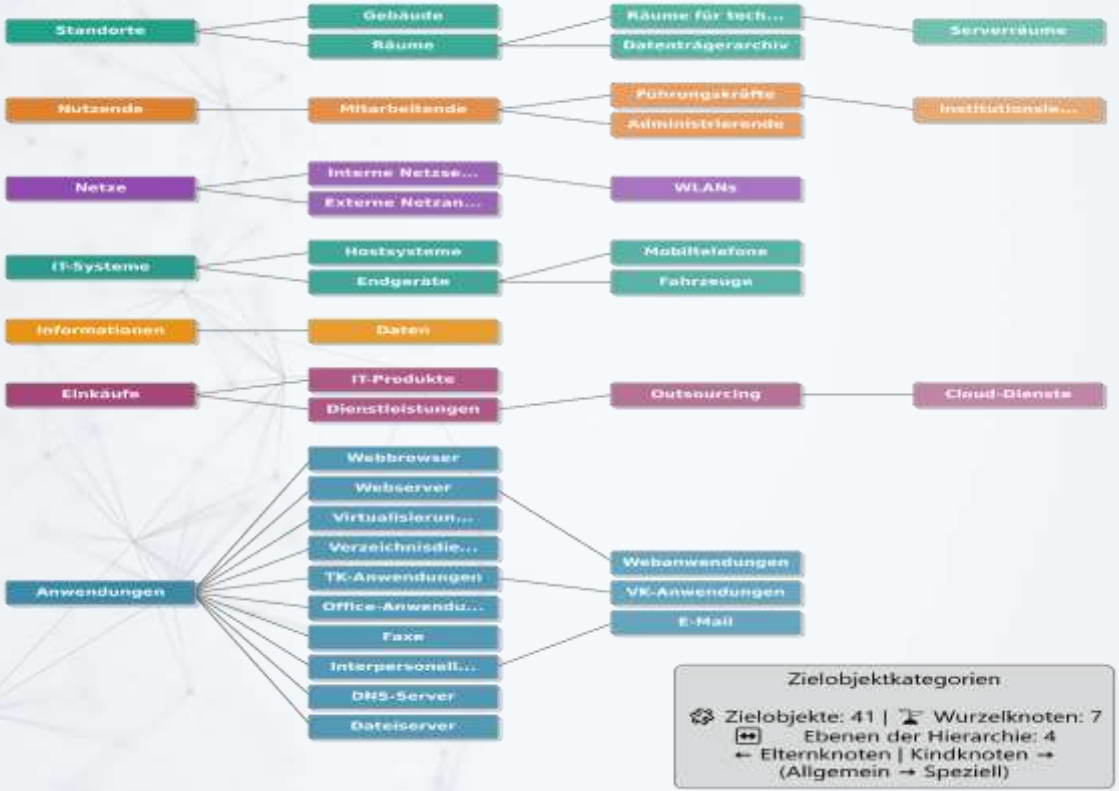
Prozessschritt 2: Anforderungsanalyse



 *Quelle: BSI

Aktueller Stand

Prozessschritt 2: Anforderungsanalyse



 *Quelle: BSI

Aktueller Stand

Prozessschritt 3: Realisierung

Analyse

- **Soll-Ist-Abgleich**
- Prüfung jeder Anforderung (Ja/Nein)
- Zusätzliche Risikobetrachtung bei „Nein“

Planung

- **Priorisierung & Maßnahmenplanung**
- Priorisierung anhand von Risiko, Aufwand & Ressourcenlage
- Festlegung von Zuständigkeiten & Fristen

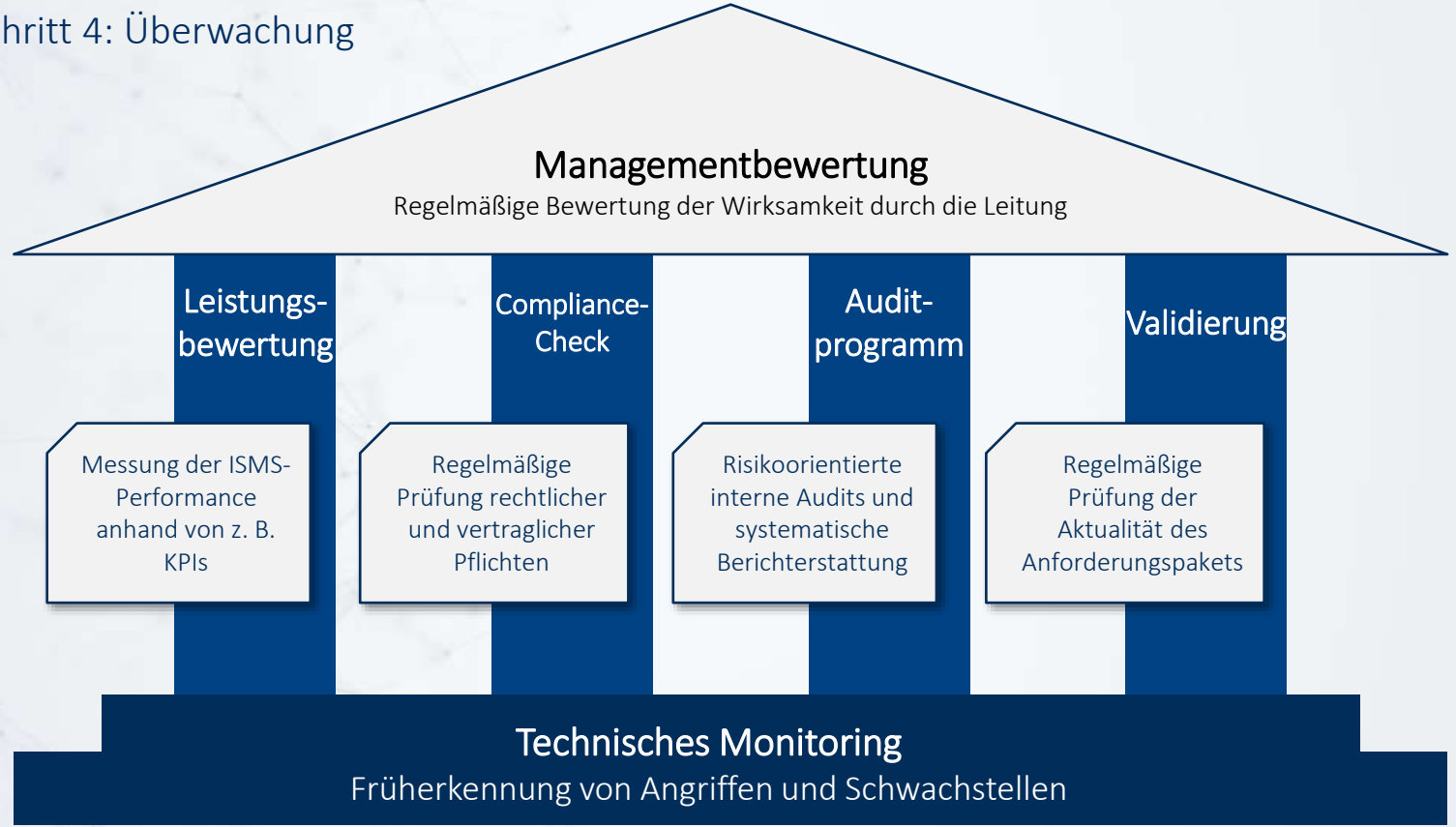
Steuerung

- **Freigabeprozess & Dokumentation**
- Risiken und Abweichungen sind durch die Leitungsebene freizugeben
- Kontinuierliche Fortschrittsverfolgung

Umsetzungszyklus

Aktueller Stand

Prozessschritt 4: Überwachung



Aktueller Stand

Prozessschritt 5: Verbesserung

Input

Reaktiv:
Ursachenanalyse von Defiziten

Proaktiv:
Nutzung von Optimierungs-potenzialen

Integration in die Realisierung

Output

Wirksamkeits-prüfung:
Validierung durch „Re-Audits“

Bewertung:
Trendanalyse des Sicherheits-niveaus

Fazit

- An vielen Stellen bleibt der Grundschutz++ dem IT-Grundschutz methodisch treu
- Praktiken, Zielobjektkategorien & die Entwicklung von Anforderungspaketen stellen die größte Herausforderung dar
- Eine Migration von IT-Grundschutz zu Grundschutz++ erscheint möglich, zum aktuellen Zeitpunkt wurde dazu vom BSI jedoch nichts veröffentlicht
- Eine signifikante „Vereinfachung“ ist vor allem bei zentralisierten Verbünden möglich
- Zukünftig ist jedoch eine deutlich stärkere Abhängigkeit von Tools eine mögliche Einstiegshürde für den Grundschutz++

HISOLUTIONS

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com

Quellen

1. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Managementsystemen/ISO-27001-Basis-IT-Grundschutz/ErteilteZertifikate/iso27001zertifikate_node.html
   Zuletzt abgerufen 08.02.2026
2. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Listen/Zertifikate-ISO-27001-auf-Basis-von-IT-Grundschutz/iso27001_zertifikate_lfd-2024.html?nn=455512
   Zuletzt Abgerufen 08.02.2026
3. https://www.ria.ee/sites/default/files/documents/2022-11/Overview-of-the-Estonian-Security-System-ISKE.pdf
   Zuletzt Abgerufen 08.02.2026
4. https://www.bundestag.de/dokumente/textarchiv/2025/kw42-pa-inneres-nis-2-1112700
   Zuletzt Abgerufen 08.02.2026
5. https://www.iit-berlin.de/wp-content/uploads/2025/02/Zukunftsradar-Digitale-Kommune-2024_iit-DStGB_WEB.pdf
   Zuletzt Abgerufen 08.02.2026