Ringvorlesung HAW 2026

BSI IT-Grundschutz

Ein Überblick über den IT-Sicherheitsstandard

Dr. iur. Lutz Gollan
Landesbetrieb Verkehr, Hamburg

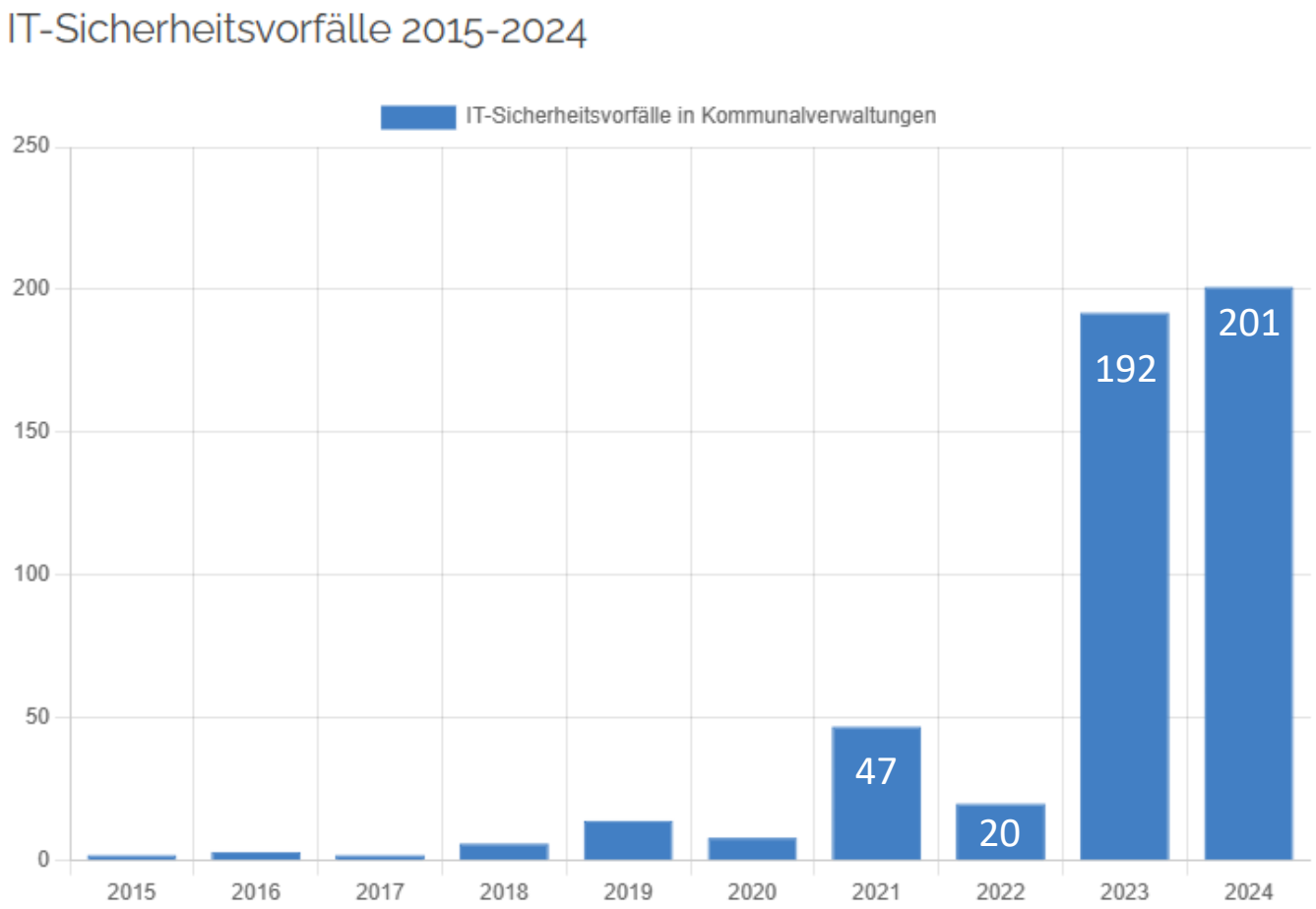
Gliederung

- Informationssicherheit und Standards
- Überblick „BSI IT-Grundschutz“
- Vorgehen und Umsetzung
- Ausblick

Die Anforderungen wachsen

- Die Abhängigkeit von IT-Systemen steigt,
- Cybercrime ist ein Geschäftsmodell, Cyber-Kriegsführung gewinnt an Bedeutung,
- IT-Umgebungen und -Nutzung sind stärker von Vernetzung geprägt (mobile Nutzung Homeoffice, Cloud, …),
- Anforderungen durch andere Institutionen, z. B. i-Kfz (KBA), KRITIS-Regelungen steigen und auch
- Naturkatastrophen nehmen zu.

Kommunale Sicherheitsvorfälle



Quelle: Jens Lange (https://kommunaler-notbetrieb.de)

Informationssicherheit

Informationssicherheit ist der Zustand, in dem die drei Sicherheitsziele

- Vertraulichkeit,
- Integrität und
- Verfügbarkeit

für Informationen jeglicher Art im für die verantwortliche Stelle erforderlichen Maße durch angemessene technische und organisatorische Maßnahmen gewährleistet werden.

Informationssicherheit – Bedingungen

- Daraus folgt, dass es einerseits Ziele gibt, deren Erreichungsgrad *messbar* ist, und
- andererseits nur *angemessene* Maßnahmen zu treffen sind.
- Die Messbarkeit kann durch *Standards* erreicht werden.
  - Standard meint ein durch ein Gremium vorgegebenes und dokumentiertes Vorgehen
  - mit Vorgaben zur Erreichung der Sicherheitsziele,
  - das nachvollziehbar dokumentiert wird.

Informationssicherheitsmanagement-System-Standard = ISMS

ISMS-Standards

Kriterien	VdS 10000	CISIS12	SiKoSH	ISO/IEC 27000-Reihe	BSI IT-Grundschutz[21]
Herausgeber	VdS Schadenverhütung GmbH	IT-Sicherheitscluster e. V.[22]	ITV.SH AöR	International Standards Organisation[23]	Bundesamt für Sicherheit in der Informationstechnik[24]
Zielgruppe	kleine und mittlere Unternehmen	kleine und mittlere Unternehmen, öffentliche Verwaltung, Hochschulen	Kommunalverwaltungen	Organisationen jeder Größenordnungen	Organisationen jeder Größenordnungen und öffentliche Verwaltung
Dokumentation	ca. 40 Seiten	Handbuch 35 Seiten, Katalog 976 Seiten, Norm 61 Seiten	Standard 50 Seiten; insgesamt ca. 70 Dokumente	ca. 400 Seiten	ca. 5.000 Seiten
Detaillierung	minimal verweisend	mittel, praxisnah	praxisnah	minimalistisch abstrakt	maximal detailliert
Aufbau	Selektierte Bausteine und Maßnahmen	Selektierte Bausteine und Maßnahmen	Bausteine und Maßnahmen der kommunalen Basisabsicherung	Maßnahmen-empfehlungen	umfassende Bausteine, Gefährdungen und Maßnahmen
Umfang des Maßnahmenkatalogs	ca. 18 Kapitel plus Anhang, ca. 100 Maßnahmen	ca. 400 Maßnahmen	entsprechend Grundschutzprofil Basisabsicherung	ca. 150 Maßnahmen	ca. 1.100 Maßnahmen

Quelle: Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen, v3.0,#verfügbar unter https://www.staedtetag.de/files/dst/docs/Themen/2024/Handreichung-ISLL-2024.pdf

ISMS-Standards

Kriterien	VdS 10000	CISIS12	SiKoSH	ISO/IEC 27000-Reihe	BSI IT-Grundschutz[21]
Herausgeber	VdS Schadenverhütung GmbH	IT-Sicherheitscluster e. V.[22]	ITV.SH AöR	International Standards Organisation[23]	Bundesamt für Sicherheit in der Informationstechnik[24]
Zielgruppe	kleine und mittlere Unternehmen	kleine und mittlere Unternehmen, öffentliche Verwaltung, Hochschulen	Kommunalverwaltungen	Organisationen jeder Größenordnungen	Organisationen jeder Größenordnungen und öffentliche Verwaltung
Dokumentation	ca. 40 Seiten	Handbuch 35 Seiten, Katalog 976 Seiten, Norm 61 Seiten	Standard 50 Seiten; insgesamt ca. 70 Dokumente	ca. 400 Seiten	ca. 5.000 Seiten
Detaillierung	minimal verweisend	mittel, praxisnah	praxisnah	minimalistisch abstrakt	maximal detailliert
Aufbau	Selektierte Bausteine und Maßnahmen	Selektierte Bausteine und Maßnahmen	Bausteine und Maßnahmen der kommunalen Basisabsicherung	Maßnahmen-empfehlungen	umfassende Bausteine, Gefährdungen und Maßnahmen
Umfang des Maßnahmenkatalogs	ca. 18 Kapitel plus Anhang, ca. 100 Maßnahmen	ca. 400 Maßnahmen	entsprechend Grundschutzprofil Basisabsicherung	ca. 150 Maßnahmen	ca. 1.100 Maßnahmen

Quelle: Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen, v3.0,#verfügbar unter https://www.staedtetag.de/files/dst/docs/Themen/2024/Handreichung-ISLL-2024.pdf

Überblick BSI IT-Grundschutz

- BSI-Standard 200-1 definiert allgemeine Anforderungen an ein Managementsystem für Informationssicherheit (ISMS)
- 200-2 bildet die Basis der Methodik mit drei Vorgehensweisen:
  - Basis-Absicherung (dazu die Vorstufe „Weg in die Basisabsicherung – WiBA“)
  - Kern-Absicherung („Kronjuwelen“)
  - Standard-Absicherung (umfassend)
- 200-3 beschreibt eine standardisierte Risikobewertung
- 200-4 ist ein Standard für ein „Business Continuity Management System“ (BCMS) – die Phase *nach* einem Sicherheitsvorfall (z.B. Wiederanlaufen der kritischen Systeme) (vgl. Folge-Vortrag)

Fokus: Basisabsicherung

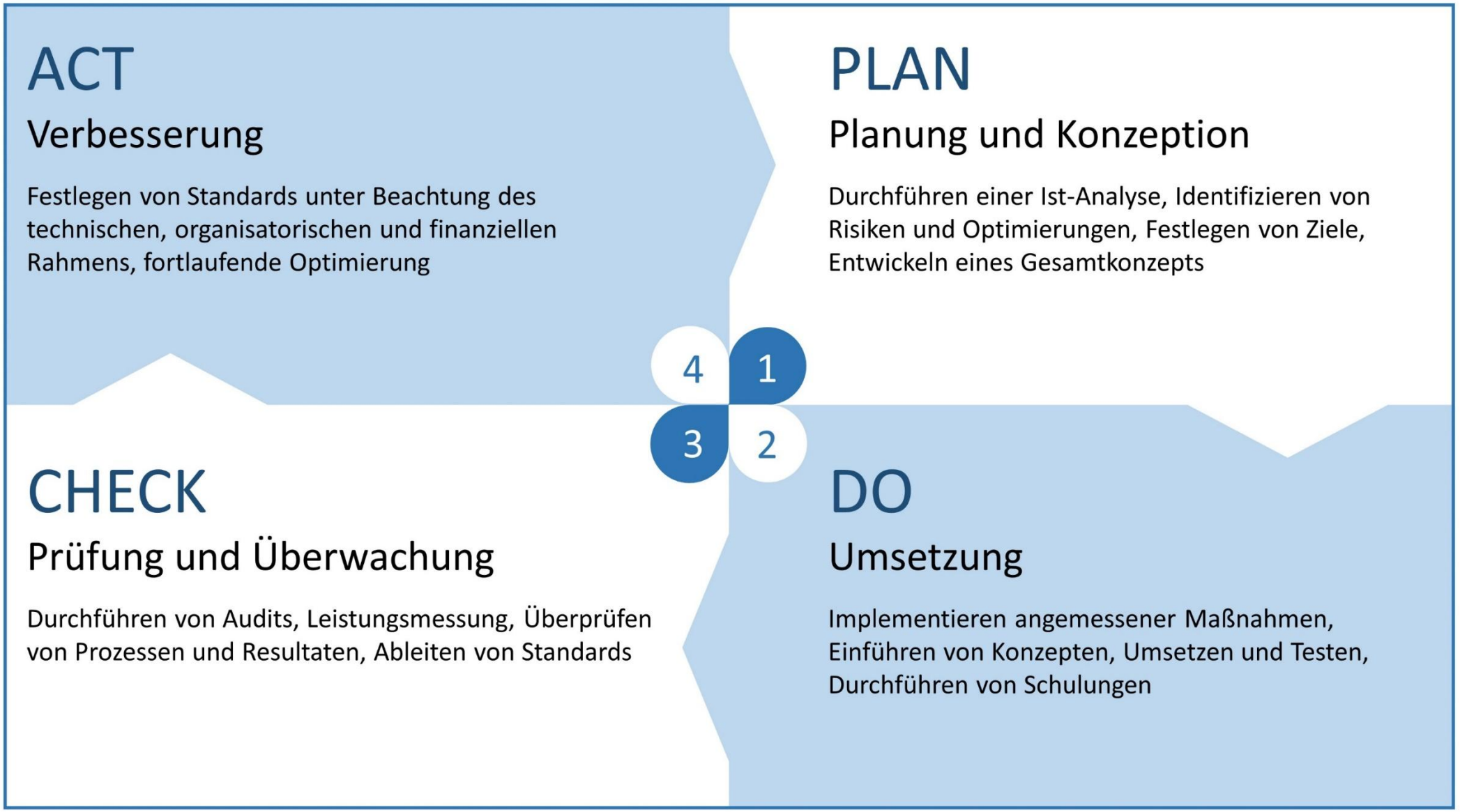
- Nach dem „Weg in die Basisabsicherung“ sollte das Ziel die Umsetzung der Basisabsicherung sein.
- Das bedeutet, dass über den gesamten sog. Informationsverbund hinweg die wichtigsten Anforderungen betrachtet und dokumentiert werden (80/20-Prinzip).
- Hilfreich sind dabei sog. IT-Grundschutzprofile, die von verschiedenen Institutionen für verschiedene Typen von Organisationen Subsets aller Bausteine und Anforderungen des „IT-Grundschutz-Kompendiums“ bereitstellen, z.B. für Hochschulen, Forschungseinrichtungen, Kommunalverwaltungen, Bundesgerichte, Papierfabriken, Reedereien

Vorgehen und Umsetzung

- BSI-Standard 200-2 sieht eine Abfolge von Schritten zum Planen („Plan“), Umsetzen („Do“), Prüfen und Überwachen („Check“) und Handeln/Verbessern („Act“) vor – PDCA.
- Dabei sollen alle Schritte auf die konkrete Organisation abgestimmt und dokumentiert werden.
- Damit kann auch – falls gewünscht – eine Zertifizierung erfolgen, z.B. nach „ISO 27001 Zertifizierung auf Basis von IT-Grundschutz“.
- Die Schritte bilden dabei einen Kreislauf – sobald „Handeln/ Verbessern“ abgeschlossen ist, beginnt das Planen des weiteren Vorgehens bzw. des erneuten Prüfens/Überwachens.

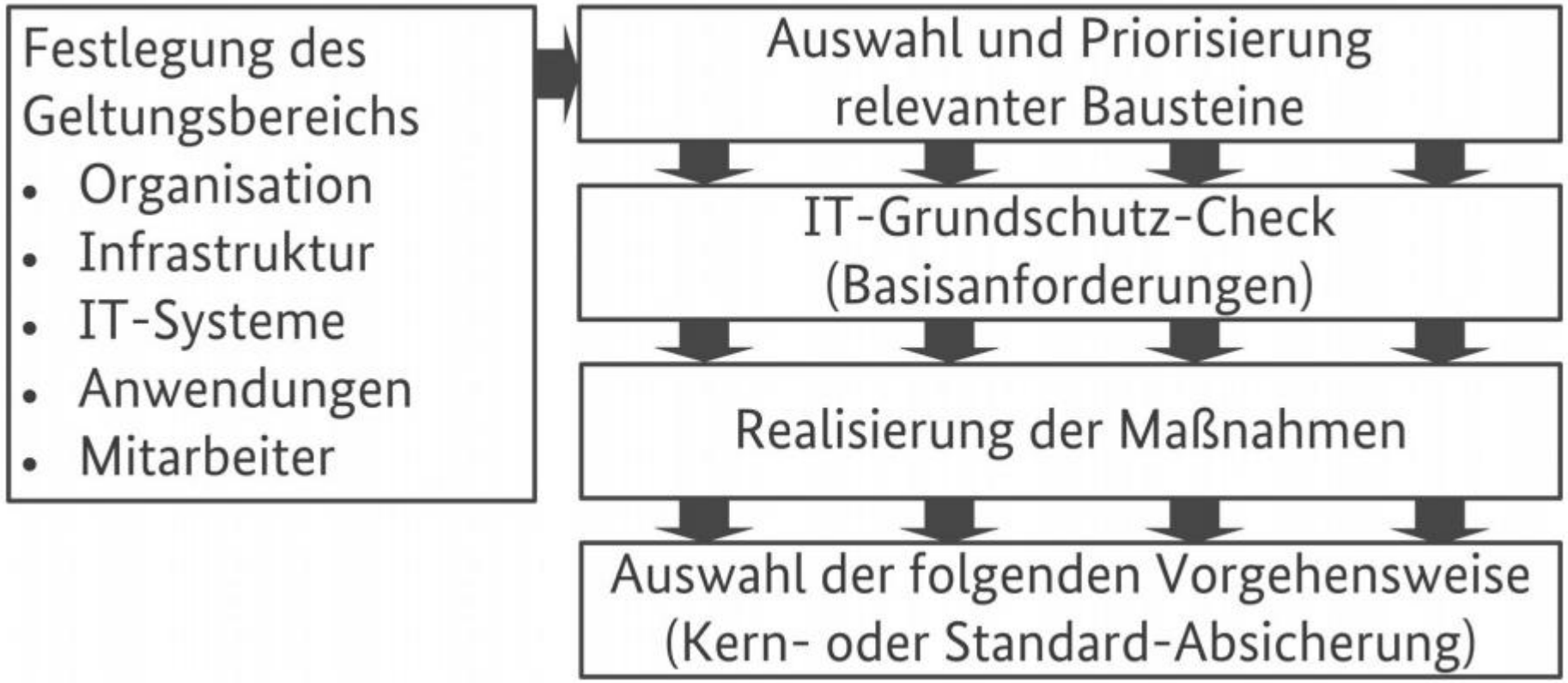
Ringvorlesung HAW 2026

PDCA-Zyklus



Quelle: Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen, v3.0,#verfügbar unter https://www.staedtetag.de/files/dst/docs/Themen/2024/Handreichung-ISLL-2024.pdf

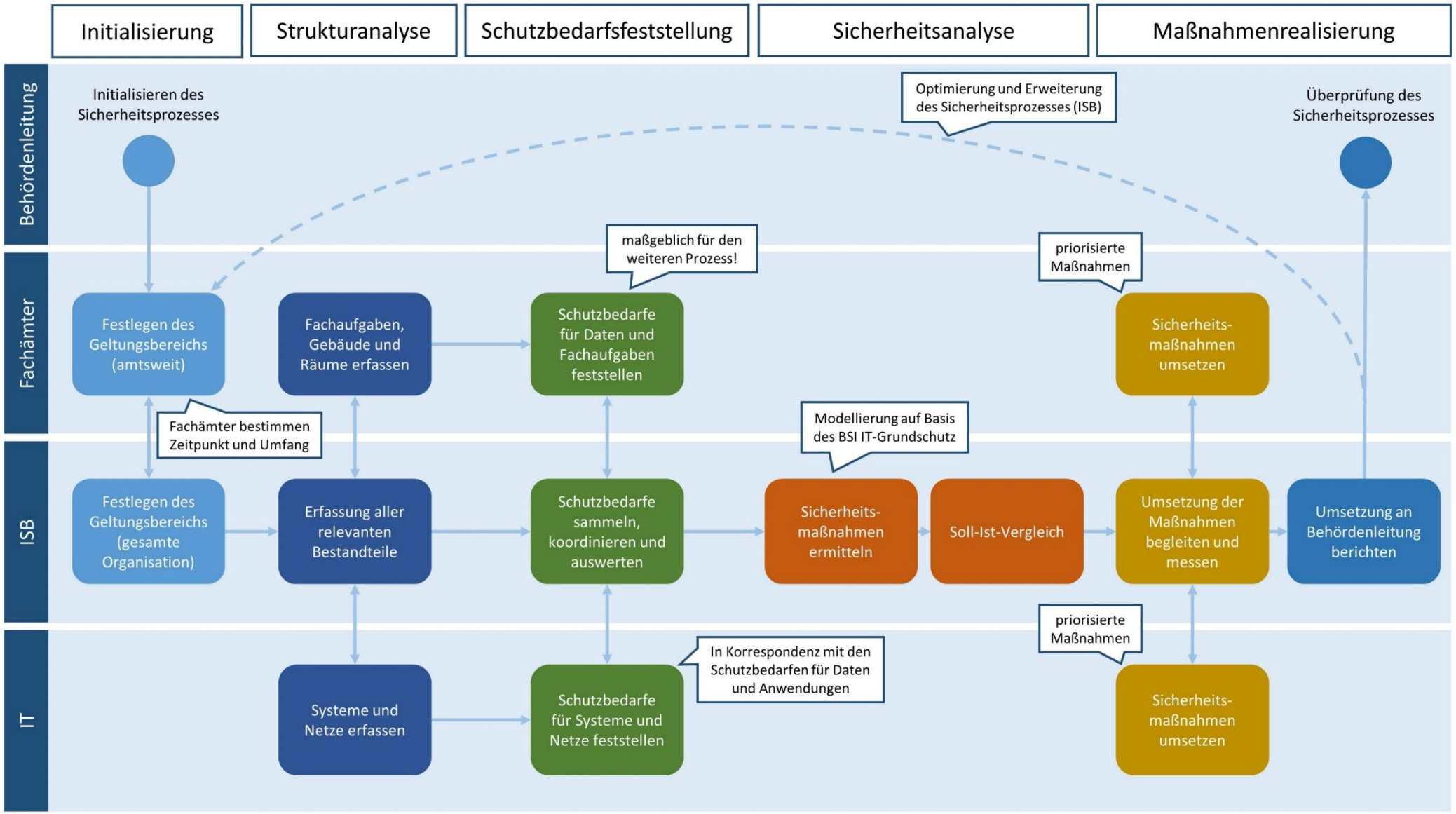
Vorgehen und Umsetzung – konkret



Quelle: BSI IT-Grundschutz 200-2, v1.0, S. 61

Ringvorlesung HAW 2026

Sicherheitsprozess

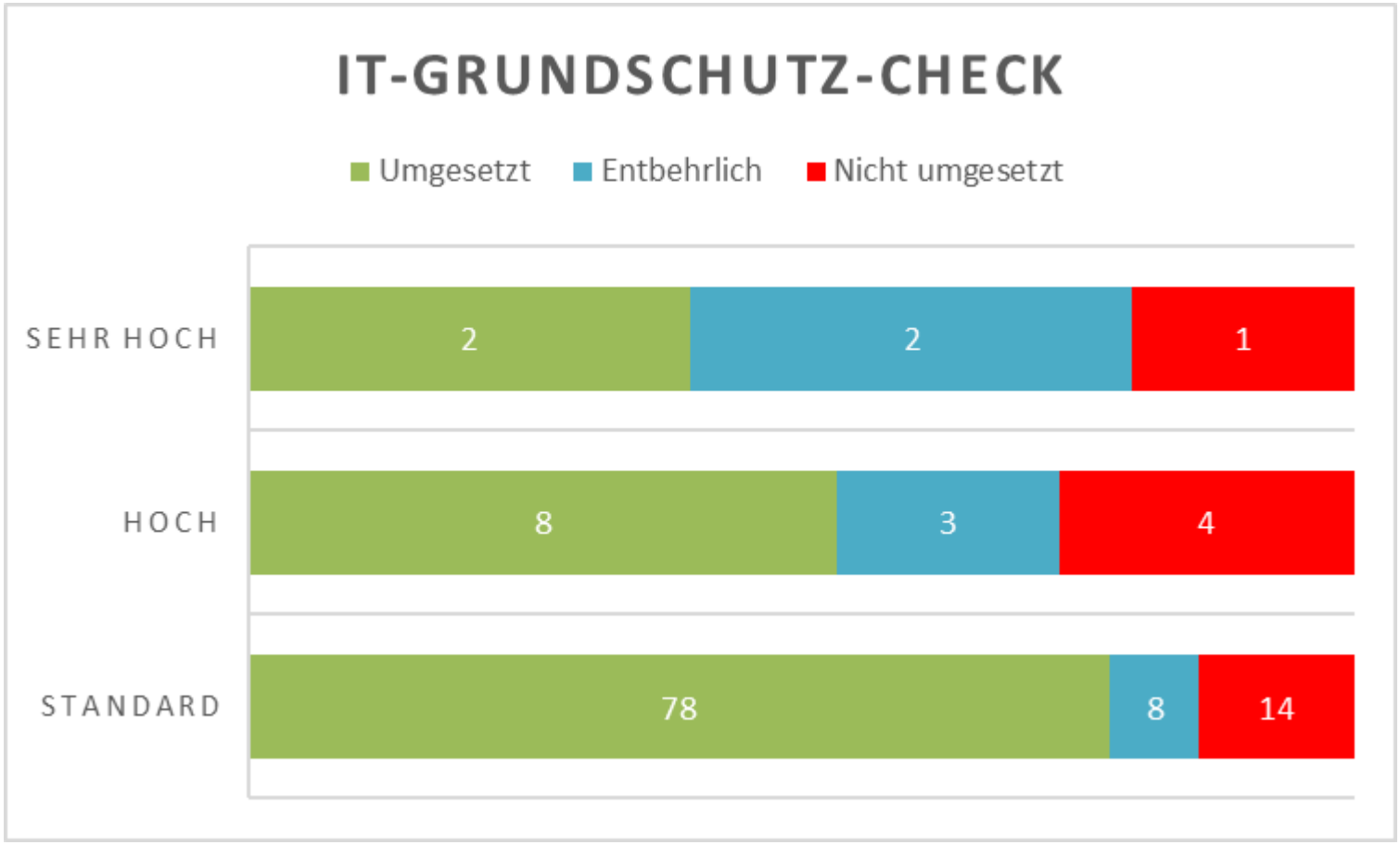


Quelle: Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen, v3.0,#verfügbar unter https://www.staedtetag.de/files/dst/docs/Themen/2024/Handreichung-ISLL-2024.pdf

Beispiel IT-Grundschutz-Check (I)

- Verschiedene Anforderungen mit verschiedenen Stufen, je nach Schutzbedarf der Informationen etc., sind auszuwählen.
- Die Anforderungen finden sich in verschiedenen Bausteinen des IT-Grundschutz-Kompendiums, z.B. OPS.1.1.1 Allgemeiner IT-Betrieb, SYS.1.2.3 Windows Server oder APP.1.1 Office-Produkte
- Auszug der Anforderungen für APP.1.1 Office-Produkte
  - APP.1.1.A2 Einschränken von Aktiven Inhalten: „Die Funktion, dass eingebettete Aktive Inhalte automatisch ausgeführt werden, MUSS deaktiviert werden."
  - APP.1.1.A12 Verzicht auf Cloud-Speicherung: „Die in einigen Office-Produkten integrierten Funktionen für Cloud-Speicher SOLLTEN grundsätzlich deaktiviert werden […]"

Beispiel IT-Grundschutz-Check (II)



BSI IT-Grundschutz++

- Mit Jahresbeginn 2026 werden insbesondere die Anforderungen schematisch und inhaltlich modernisiert.
- Die Anforderungen sollen maschinenlesbar (über GitHub), atomarer und leichter auswertbar über Leistungskennzahlen werden.
- Statt Fließtext werden die Anforderungen als strukturierte Sätze dargestellt („GOV.4.2: Die Governance MUSS einer Person die Rolle ISB zuweisen.“).
- Die Anforderungen werden sechs Prioritätsstufen zugewiesen („Zwingend“ bis „Zusätzlich für hohen Schutzbedarf“).
- Die Aktualisierungen sollen laufend, nicht jährlich erfolgen.
- …

Vielen Dank für die Aufmerksamkeit.

Kontakt: Lutz.Gollan@lbv.hamburg.de, 040-42858-2020

Gollan, L. (2021). Informationssicherheit – Grundlagen für Bibliotheken: Praxis-Überblick über den IT-Grundschutz-Standard. *API Magazin*, *2*(1). https://doi.org/10.15460/apimagazin.2021.2.1.64

Gollan, L. (2023). Technischer Datenschutz: Datensicherheit. In: Zilkens/Gollan, Datenschutz in der Kommunalverwaltung. 6. Auflage, Erich-Schmidt-Verlag.