

Grundschutz++

Know-how to go

HiSolutions AG

Sebastian Reinhardt

Agenda



- Nachlese zur it-sa
- Vorgehen nach BSI-Standard 300-1
- OSCAL und Umstieg
- 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
- ISC2 CISSP
- Zertifizierter Lead Auditor ISO 27001
- Zertifizierter PRINCE2® Practitioner
- Information Security Officer (TÜV)
- Chief Information Security Officer (TÜV)

© HiSolutions 2026

Nachlese zur it-sa

Was in Nürnberg zu hören war

1

Standard veröffentlicht

BSI-Standard 300-1 „Methodik Grundschutz++“ liegt in Version 1.0 vor

2

Arbeit geht weiter

Das BSI hat angekündigt, den Grundschutz++ weiterzuentwickeln

3

Weitere Standards folgen

Weitere Standards sollen integriert werden, insbesondere der BSI-Standard 200-4

Aus der Praxis Ein Pilotanwender berichtete von rund 130 Personentagen Aufwand. Im Unternehmen befassen sich 18 Personen mit dem Thema, 5 waren direkt an der Umsetzung beteiligt.

© HiSolutions 2026

Nachlese zur it-sa

Was vorliegt und was noch kommt

Veröffentlicht

- BSI-Standard 300-1, Version 1.0 vom 20.10.2026
- Anwenderkatalog Grundschutz++ (GS++) in der Stand-der-Technik-Bibliothek
- Zuordnung IT-Grundschutz 2023 zu GS++ als Entwurf

Angekündigt

- 30.11.2026 Schulungskonzepte für GS++-Praktiker und GS++-Berater
- Dezember 2026 Anwendungsbeispiel „BDIT“
- 26.02.2027 Konzept zur Leistungsmessung
- 31.03.2027 Leistungskennzahlen für Methodik-Anforderungen

Im Meilensteinplan ohne Termin

- Integration des BSI-Standards 200-4

© HiSolutions 2026

Nachlese zur it-sa

Meilensteinplan des BSI, Stand Oktober 2026

2026

- **01.04.2026** – Start der Pilotierungsphase
- **31.08.2026** – Ende der Pilotierungsphase
- **27.10.2026** – Vorstellung des BSI-Standards 300-1 auf der it-sa

heute, 16.11.2026

- **30.11.2026** – Schulungskonzepte für GS++-Praktiker und GS++-Berater
- **Dezember 2026** – Anwendungsbeispiel anhand der Beispielbehörde „BDIT“

2027 und später

- **01.01.2027** – Grundschutz++ ist zertifizierbar
- **1. Quartal 2027** – Start der Early-Adopter-Phase, Fortbildung für zertifizierte Berater und Auditteamleiter
- **26.02.2027** – Konzept zur Leistungsmessung in die Methodik integriert
- **31.03.2027** – Leistungskennzahlen für Anforderungen der Methodik-Praktiken
- **31.12.2027** – Ende der Early-Adopter-Phase
- **2027 ff.** – Internationalisierung, Integration anderer Managementsysteme
- **30.11.2031** – **Ende der Zertifizierbarkeit nach IT-Grundschutz**

© HiSolutions 2026

Nachlese zur it-sa

Was der Standard neu regelt

Kap. 3.2

Abhängigkeiten

Dokumentation je nach Schutzbedarf. Bei normalem genügen Anwendung zu IT-System und IT-System zu Raum

Kap. 3.3

Blaupausen

Vorgefertigte Anforderungskataloge für typische Szenarien, mit festen Parametern

Kap. 4.3

Nachweise je Maßnahme

Anforderung, Datum und prüfende Person, bei automatisierter Prüfung auch Tool und Ergebnis

Anhang 2

Geschäftsprozessanalyse

Vereinfachtes Verfahren mit fünf Mindestangaben je Geschäftsprozess

Anhang 3

Mindestkriterien

35 Kriterien für die Risikobetrachtung, von der Initiierung bis zur jährlichen Überprüfung

Anhang 4

Elementare Gefährdungen

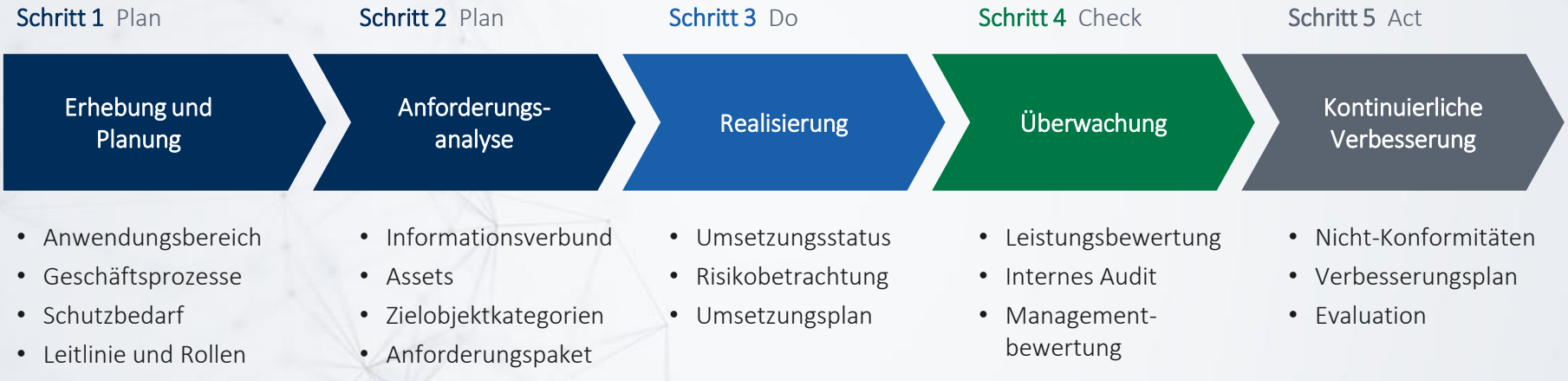
47 Gefährdungen, im Katalog jeder Anforderung per G0-Kennung zugeordnet

Einheitliche Vorgaben zur Leistungsbewertung stehen laut Kap. 5.1 noch aus. Bis dahin gestalten Institutionen sie selbst.

© HiSolutions 2026

Vorgehen nach BSI-Standard 300-1

Fünf Prozessschritte im PDCA-Zyklus



- Anwendungsbereich
- Geschäftsprozesse
- Schutzbedarf
- Leitlinie und Rollen

- Informationsverbund
- Assets
- Zielobjektkategorien
- Anforderungspaket

- Umsetzungsstatus
- Risikobetrachtung
- Umsetzungsplan

- Leistungsbewertung
- Internes Audit
- Management-bewertung

- Nicht-Konformitäten
- Verbesserungsplan
- Evaluation

© HiSolutions 2026

Vorgehen nach BSI-Standard 300-1

Ausgangspunkt sind die Geschäftsprozesse

Start | Schutzbedarf | Assets | Zielobjekte | Paket | Status | Behandeln | Freigabe

Prozesse	**Antragsbearbeitung** Geschäftsprozess	**Personalverwaltung** Geschäftsprozess	**Website Betrieb** Geschäftsprozess
Anwendungen			
IT-Systeme	Assets folgen in der Phase „Assets“		
Netze			
Räume			

Anforderungspaket

noch leer

Umsetzungsstatus

Umsetzungsplan

Risikoregister

Prozessschritt 1 Drei Geschäftsprozesse einer Beispielbehörde im Anwendungsbereich, noch ohne Bewertung. Fehlt eine Prozesslandkarte, genügt die vereinfachte Geschäftsprozessanalyse. (Kap. 2.5, Anhang 2)

© HiSolutions 2026

Vorgehen nach BSI-Standard 300-1

Schutzbedarf je Geschäftsprozess feststellen

Start | **Schutzbedarf** | Assets | Zielobjekte | Paket | Status | Behandeln | Freigabe

Prozesse	**Antragsbearbeitung** Schutzbedarf hoch	**Personalverwaltung** Schutzbedarf normal	**Website** Schutzbedarf normal
Anwendungen			
IT-Systeme	Assets folgen in der Phase „Assets“		
Netze			
Räume			

Anforderungspaket

noch leer

Umsetzungsstatus

Umsetzungsplan

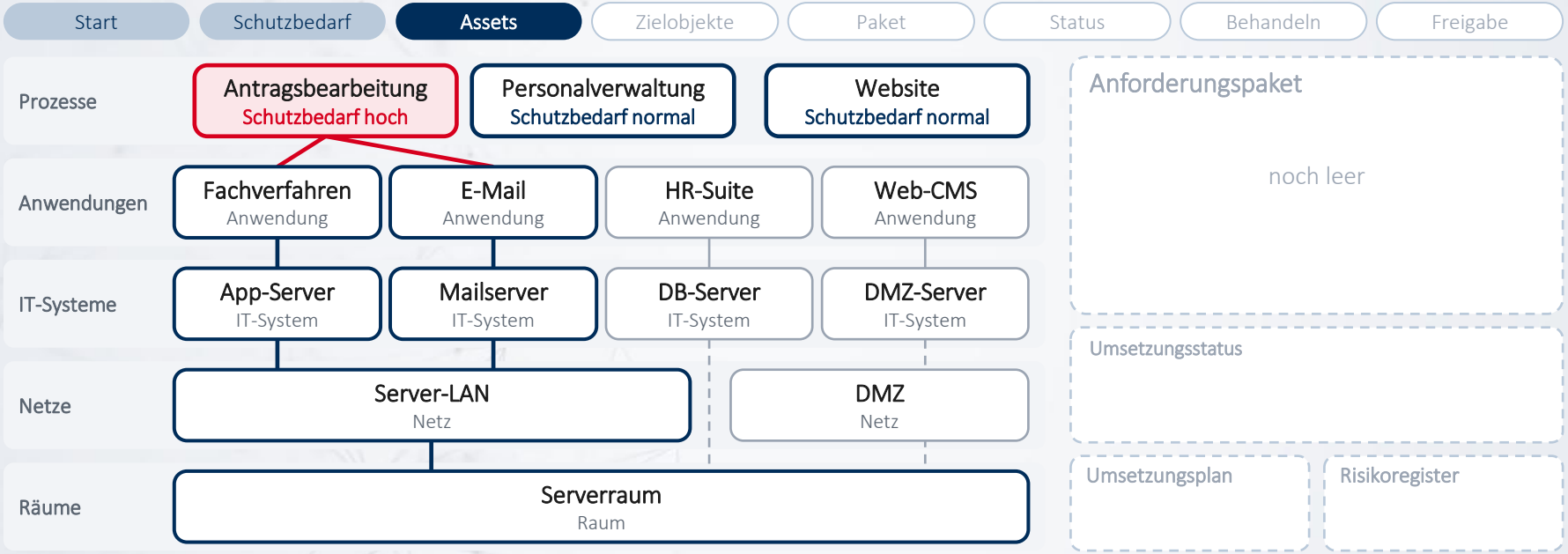
Risikoregister

Prozessschritt 1 Der Standard gibt zwei Kategorien vor, normal und hoch. Die Leitung gibt den Schutzbedarf frei. Empfohlener Einstieg ist der wichtigste Prozess der höchsten Kategorie. (Kap. 2.6, 2.10)

© HiSolutions 2026

Vorgehen nach BSI-Standard 300-1

Assets erfassen und Abhängigkeiten dokumentieren

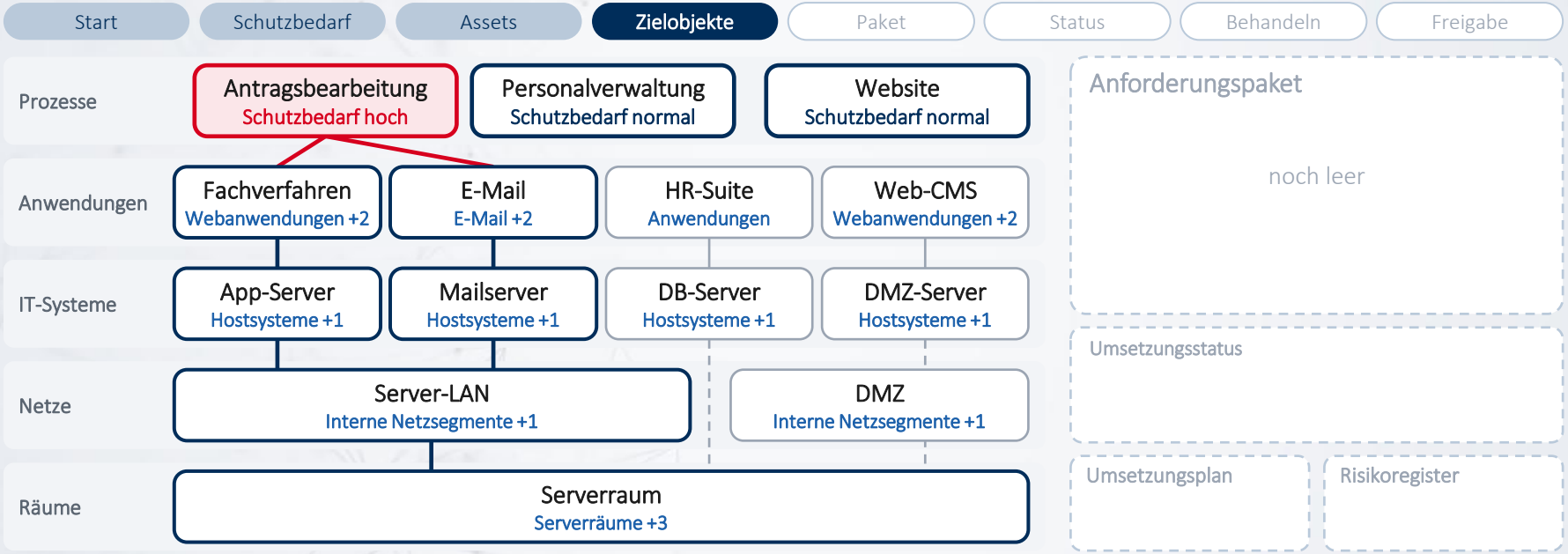


Prozessschritt 2 Bei hohem Schutzbedarf sind die Abhängigkeiten vom Prozess bis zum Raum zu dokumentieren. Bei normalem Schutzbedarf genügen Anwendung zu IT-System und IT-System zu Raum. (Kap. 3.2)

© HiSolutions 2026

Vorgehen nach BSI-Standard 300-1

Assets den Zielobjektkategorien zuordnen



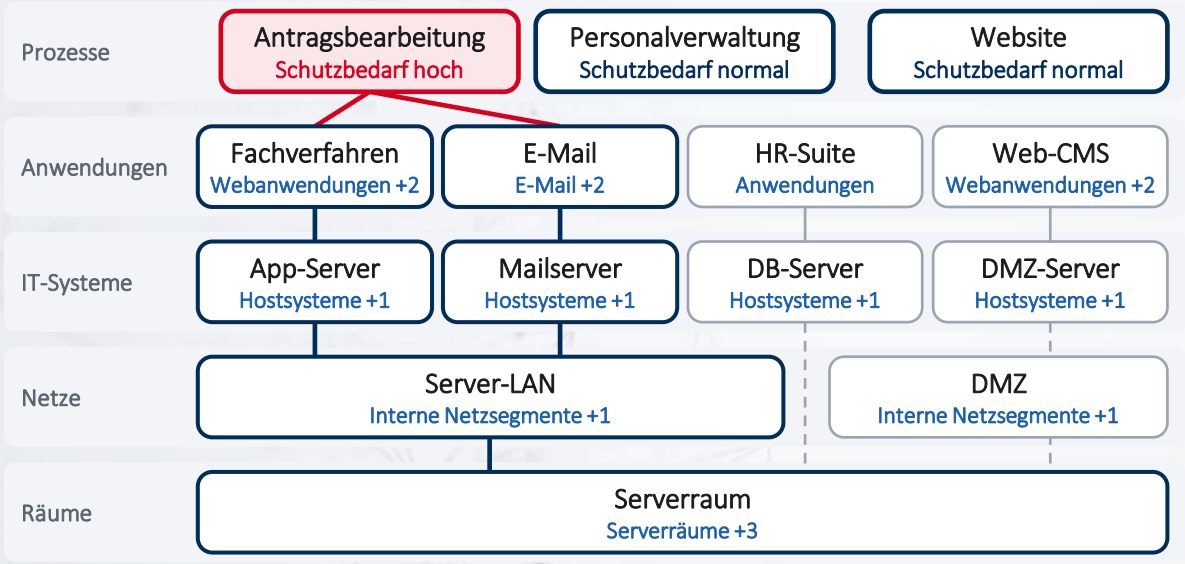
Prozessschritt 2 Jedes Asset erhält mindestens eine Zielobjektkategorie. Die übergeordneten Kategorien gelten mit, im Bild als „+n“ markiert. (Kap. 3.4.2, Anhang 1)

© HiSolutions 2026

Vorgehen nach BSI-Standard 300-1

Anforderungspaket zusammenstellen

Start | Schutzbedarf | Assets | Zielobjekte | **Paket** | Status | Behandeln | Freigabe



Anforderungspaket

Methodik-Praktiken | Ohne Kategoriebezug

immer enthalten

Anwendungen +4 | IT-Systeme +1

Netze +1 | Standorte +3

aus 13 Zielobjektkategorien für 11 Assets

Umsetzungsstatus

Umsetzungsplan

Risikoregister

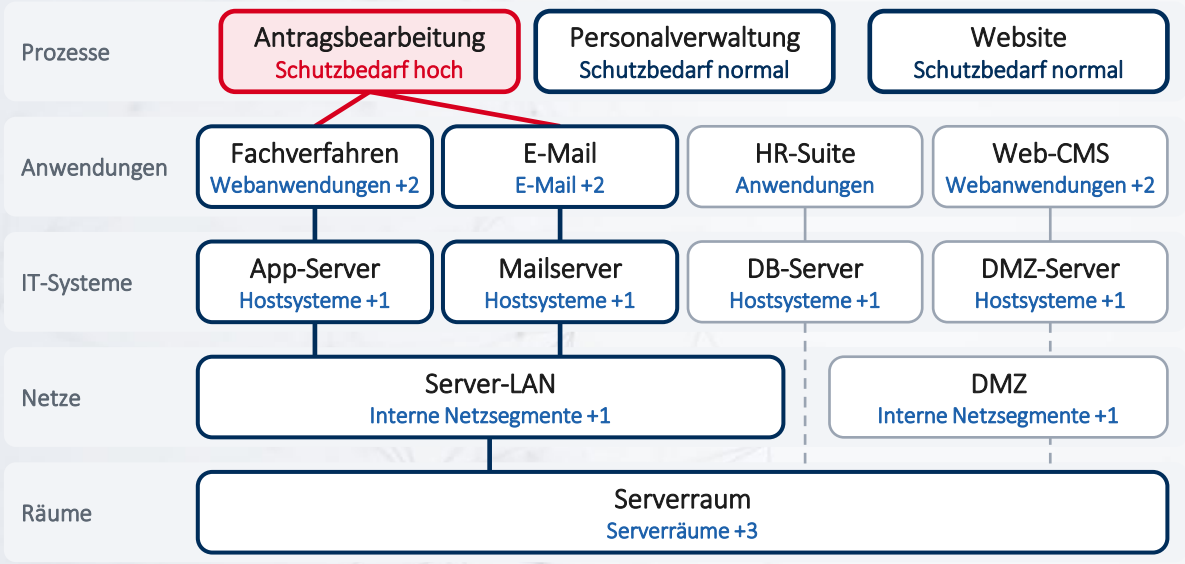
Prozessschritt 2 Methodik-Anforderungen und Anforderungen ohne Kategoriebezug sind immer enthalten. Der Rest folgt aus der Zuordnung, gleiche Anforderungen zählen einmal. (Kap. 3.4)

© HiSolutions 2026

Vorgehen nach BSI-Standard 300-1

Umsetzungsstatus je Anforderung ermitteln

Start | Schutzbedarf | Assets | Zielobjekte | Paket | **Status** | Behandeln | Freigabe



Anforderungspaket

Methodik-Praktiken | Ohne Kategoriebezug

immer enthalten

Anwendungen +4 | IT-Systeme +1

Netze +1 | Standorte +3

aus 13 Zielobjektkategorien für 11 Assets

Umsetzungsstatus, Beispiel



Umsetzungsplan

Risikoregister

erfüllt | nicht anwendbar | MUSS offen

SOLLTE temporär offen | SOLLTE dauerhaft offen

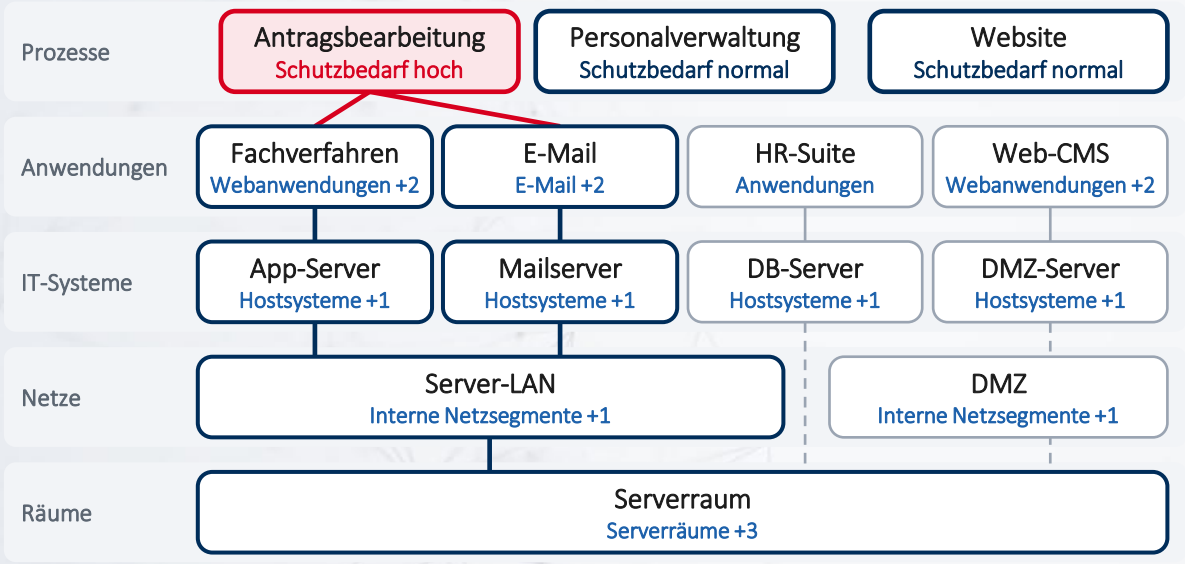
Prozessschritt 3 Jede Anforderung erhält einen von drei Status. „Nicht anwendbar“ braucht eine Begründung. (Kap. 4.1.1)

© HiSolutions 2026

Vorgehen nach BSI-Standard 300-1

Offene Anforderungen behandeln

Start | Schutzbedarf | Assets | Zielobjekte | Paket | Status | **Behandeln** | Freigabe



Anforderungspaket

Methodik-Praktiken | Ohne Kategoriebezug

immer enthalten

Anwendungen +4 | IT-Systeme +1

Netze +1 | Standorte +3

aus 13 Zielobjektkategorien für 11 Assets

Umsetzungsstatus, Beispiel



Umsetzungsplan

6 Maßnahmen

Risikoregister

2 Auslöser

erfüllt | nicht anwendbar | MUSS offen

SOLLTE temporär offen | SOLLTE dauerhaft offen

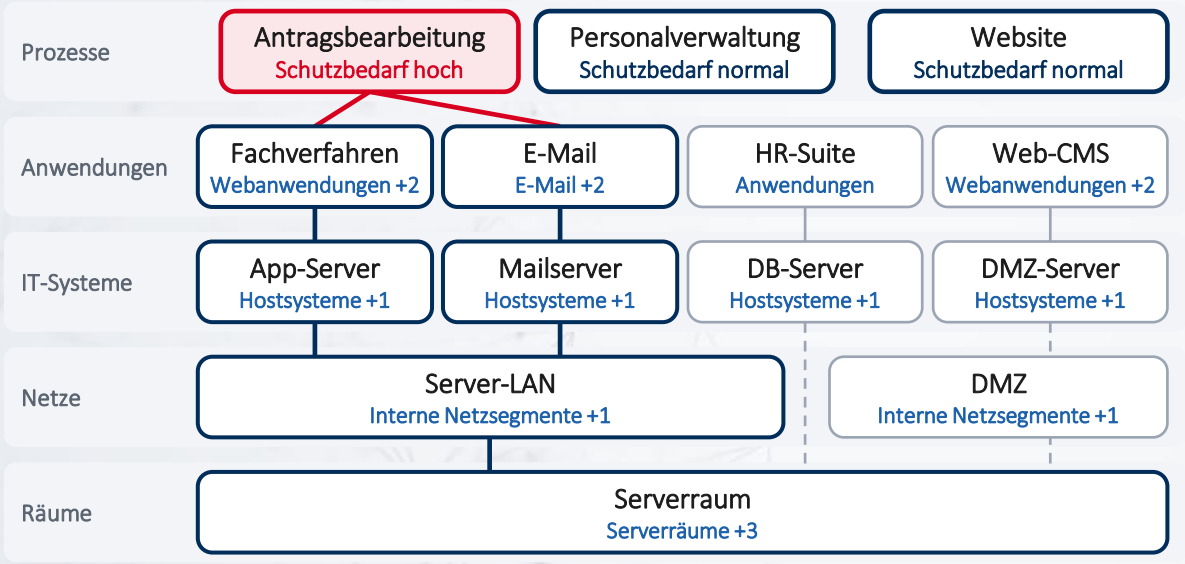
Prozessschritt 3 MUSS und temporär offene SOLLTE gehen in den Umsetzungsplan. Dauerhaft offene SOLLTE und hoher Schutzbedarf lösen eine Risikobetrachtung aus. (Kap. 4.1.2, 4.2)

© HiSolutions 2026

Vorgehen nach BSI-Standard 300-1

Restrisiken und Umsetzungsplanung freigeben

Start | Schutzbedarf | Assets | Zielobjekte | Paket | Status | Behandeln | **Freigabe**



Anforderungspaket

Methodik-Praktiken | Ohne Kategoriebezug

immer enthalten

Anwendungen +4 | IT-Systeme +1

Netze +1 | Standorte +3

aus 13 Zielobjektkategorien für 11 Assets

Umsetzungsstatus, Beispiel



Umsetzungsplan

6 freigegeben

Risikoregister

2 freigegeben

erfüllt | nicht anwendbar | MUSS offen

SOLLTE temporär offen | SOLLTE dauerhaft offen

Prozessschritt 3 Die Institutionsleitung gibt die Restrisiken frei. Die Risikoeigentümer autorisieren die Umsetzungsplanung. (Kap. 4.2.3)

© HiSolutions 2026

Vorgehen nach BSI-Standard 300-1

Anforderung nicht erfüllt, was nun?

Status je Anforderung

erfüllt | nicht erfüllt | nicht anwendbar, mit Begründung

Das Modalverb entscheidet über das weitere Vorgehen

MUSS

- Maßnahme festlegen und umsetzen
- Keine Risikoakzeptanz
- Keine Ausnahme-genehmigung

SOLLTE, temporär offen

- Erfüllung ist geplant
- Stichhaltig begründen
- Leitung trägt das Risiko bis zur Umsetzung

SOLLTE, dauerhaft offen

- Risikobetrachtung durchführen
- Elementare Gefährdungen berücksichtigen
- Leitung gibt Restrisiken frei

KANN

- Umsetzung optional
- Sicherheitsniveau „erhöht“
- Hilft bei der Risiko-betrachtung

Häufen sich dauerhaft offene SOLLTE-Anforderungen, kann in einer Zertifizierung eine erhebliche Abweichung festgestellt werden.

© HiSolutions 2026

Vorgehen nach BSI-Standard 300-1

Eigene Risikobetrachtung in drei Fällen

Bei normalem Schutzbedarf ist keine eigene Risikobetrachtung nötig. Dem Anwenderkatalog liegt eine allgemeine Risikobetrachtung des BSI zugrunde.

1. **Hoher Schutzbedarf**
   Ein Geschäftsprozess hat bei mindestens einem Schutzziel hohen Schutzbedarf
2. **Nicht abgedecktes Asset**
   Zielobjektkategorien und ihre Anforderungen decken ein relevantes Asset nicht hinreichend ab
3. **Dauerhaft offene SOLLTE-Anforderung**
   Eine anwendbare Anforderung wird auf absehbare Zeit oder endgültig nicht erfüllt

35 Mindestkriterien in Anhang 3

- Verfahren frei wählbar, zum Beispiel ISO/IEC 27005 oder ISO 31000
- Risiken vorrangig auf Ebene der Geschäftsprozesse
- Risikoeigentümer ist der Eigentümer des Geschäftsprozesses, sofern nichts anderes festgelegt ist
- Überprüfung mindestens jährlich und bei wesentlichen Änderungen

© HiSolutions 2026

Vorgehen nach BSI-Standard 300-1

Überwachen und verbessern

Prozessschritt 4, Überwachung (Check)

- Leistungsbewertung des ISMS
- Internes Auditprogramm
- Managementbewertung durch die Leitung
- Monitoring von Vorfällen, Schwachstellen und Bedrohungen
- Validierung der Anforderungen

Prozessschritt 5, kontinuierliche Verbesserung (Act)

- Nicht-Konformitäten mit Ursachenanalyse
- Verbesserungspotenziale identifizieren
- Korrektur- und Verbesserungsplan geht in den Umsetzungsplan ein
- Evaluation der Wirksamkeit

Einheitliche Vorgaben zur Leistungsbewertung stehen noch aus. Der Meilensteinplan nennt dafür den 26.02.2027 und den 31.03.2027.

© HiSolutions 2026

OSCAL und Umstieg

OSCAL transportiert Anforderungen, die Methodik bleibt Grundschutz

BSI

Pflegt den Anwenderkatalog in der Stand-der-Technik-Bibliothek

OSCAL

ISMS-Tool

Liest den Katalog ein und zeigt Anforderungen, Status und Nachweise

Anforderungen

Anwender

Arbeiten nach BSI-Standard 300-1 mit ihrem Anforderungspaket

OSCAL ist ein Datenformat

Die Open Security Controls Assessment Language (OSCAL) legt fest, wie Kataloge und Anforderungen strukturiert abgelegt werden.

300-1 kommt ohne OSCAL aus

Der Text des Standards erwähnt das Format nicht. Die fünf Prozessschritte gelten unabhängig vom Werkzeug.

Mehr OSCAL ist möglich

Weitere OSCAL-Modelle lassen sich nutzen. Die Methodik des Grundschutz++ verlangt es nicht.

© HiSolutions 2026

OSCAL und Umstieg

Eine Anforderung, zwei Ansichten

So lesen Sie die Anforderung

RISK.1.1

Risikomanagement **MUSS** einheitliche Methoden nach **einem anerkannten Standard** verankern.

Praktik	Risikomanagement
Modalverb	MUSS
Parameter	einem anerkannten Standard

So liest sie das Tool

```
{
  "id": "RISK.1.1",
  "params": [{
    "id": "risk.1.1-prm1",
    "label": "einem anerkannten Standard"
  }],
  "parts": [{
    "name": "statement",
    "prose": "Risikomanagement MUSS
      einheitliche Methoden nach
      {{ insert: param, risk.1.1-prm1 }}
      verankern."
  }]
}
```


© HiSolutions 2026

OSCAL und Umstieg

Was aus dem IT-Grundschutz weiter trägt

Bisher im IT-Grundschutz	Künftig nach BSI-Standard 300-1	Einschätzung
Strukturanalyse	Assets mit Abhängigkeiten erfassen (Kap. 3.2)	● Weitgehend nutzbar, Bezug zu Geschäftsprozessen ergänzen
Schutzbedarfsfeststellung	Schutzbedarf je Geschäftsprozess, normal oder hoch (Kap. 2.6)	● Vom Prozess her neu aufsetzen, eigene Kategorien abbilden
Modellierung mit Bausteinen	Assets den Zielobjektkategorien zuordnen (Kap. 3.4.2)	● Neu zuordnen, die Asset-Liste bleibt Grundlage
IT-Grundschutz-Check	Umsetzungsstatus je Anforderung (Kap. 4.1)	● Neu bewerten, „teilweise“ entfällt
Risikoanalyse nach BSI-Standard 200-3	Risikobetrachtung (Kap. 4.2, Anhang 3)	● Methode gegen die 35 Mindestkriterien prüfen
Realisierungsplan	Umsetzungsplan mit Nachweisen (Kap. 4.3)	● Übernehmen, Nachweise je Maßnahme ergänzen

● weitgehend nutzbar ● anpassen ● neu erarbeiten

© HiSolutions 2026

OSCAL und Umstieg

Der Aufwand liegt im Übertragen

IT-Grundschutz 2023, Auswahl

NET.1.1
… MUSS eine spezifische Sicherheitsrichtlinie für das Netz erstellt werden.

INF.14
Für die Übergänge zwischen den Segmenten SOLLTEN entsprechende Regeln definiert … werden.

APP.3.6
Es MUSS zuerst festgelegt werden, wie der Netzdienst DNS aufgebaut werden soll.

Grundschutz++

Praktik Architektur

Architektur MUSS Verfahren und Regelungen zur Architektur des Netzes und damit verbundener Infrastrukturen verankern.

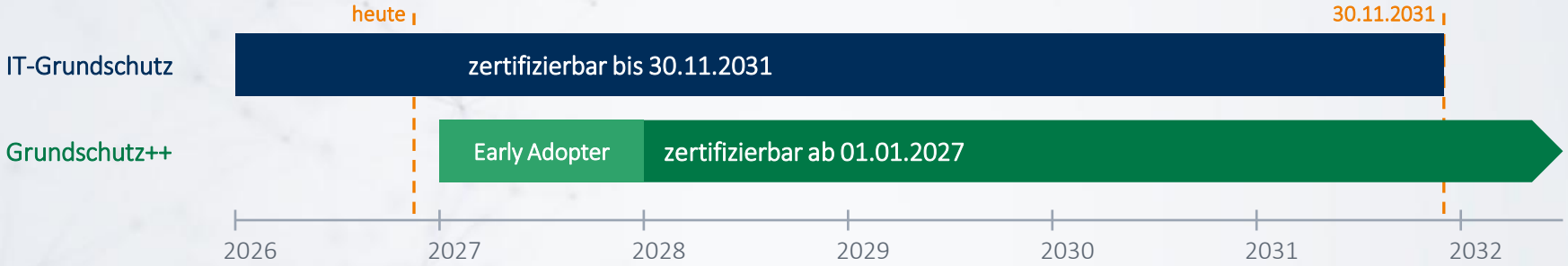
Für die Planung

1. Umsetzungsstand je Anforderung neu bewerten
2. Zuordnungstabelle des BSI als Einstieg nutzen, sie liegt als Entwurf vor
3. Aufwand realistisch ansetzen. Ein Pilotanwender nannte rund 130 Personentage

© HiSolutions 2026

OSCAL und Umstieg

Wann umsteigen?



1 Bestehendes Zertifikat

Umstieg mit einer Rezertifizierung planen, spätestens mit der letzten vor dem 30.11.2031

2 Jetzt vorbereiten

Geschäftsprozesse und Schutzbedarf erheben, Asset-Liste auf Zielobjektkategorien abbilden

3 Im Blick behalten

Auditierungsschema und Übergangsregeln für laufende Zertifikate stehen nicht im Meilensteinplan

© HiSolutions 2026

Fazit

Was Sie mitnehmen sollten

01

Der Standard liegt vor

BSI-Standard 300-1 liegt in Version 1.0 vor. Schulungskonzepte, Anwendungsbeispiel und Leistungsmessung folgen laut Meilensteinplan bis März 2027.

02

Geschäftsprozesse zuerst

Der Schutzbedarf je Prozess, normal oder hoch, steuert Dokumentationstiefe und Risikobetrachtung.

03

OSCAL ist das Transportmittel

Die Anforderungen kommen maschinenlesbar. Gearbeitet wird nach der Methodik des Grundschutz++.

04

Der Umstieg braucht Planung

IT-Grundschutz bleibt bis 30.11.2031 zertifizierbar. Der Umsetzungsstand ist je Anforderung neu zu bewerten.

© HiSolutions 2026

Early Adopter werden?

HiSolutions begleitet Ihr Projekt

Die Early-Adopter-Phase läuft 2027. Wir begleiten Institutionen, die früh nach **BSI-Standard 300-1** arbeiten wollen.

01 **Standortbestimmung**

Abgleich Ihres ISMS mit dem BSI-Standard 300-1 und Fahrplan für den Umstieg

02 **Umsetzung**

Geschäftsprozesse, Schutzbedarf, Anforderungspaket und Umsetzungsplan gemeinsam erarbeiten

03 **Weg zum Zertifikat**

Internes Audit und Vorbereitung auf die Zertifizierung auf Basis von Grundschutz++

Sprechen Sie uns an

Sebastian Reinhardt
Senior Expert IT-Grundschutz

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

© HiSolutions 2026



HISOLUTIONS

Schloßstraße 1 | 12163 Berlin

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

www.hisolutions.com

© HiSolutions AG