Kurzanleitung für die Erstellung eines Sicherheitskonzeptes

Basis-Absicherung – Nach Bundesamt für Sicherheit in der Informationstechnik (BSI)

Januar 2026

/ Für die öffentliche Hand von morgen /

Um ein Sicherheitskonzept nach Basis-Absicherung des BSI zu erstellen, müssen mehrere Schritte durchlaufen werden.

Was ist eine Strukturanalyse und wie wird sie durchgeführt? (1/2)

Strukturanalyse	Modellierung	IT-Grundschutz-check	Umsetzungs-planung	Sicherheitskonzept zusammenfügen

Definition:

Die **Strukturanalyse bündelt** die sogenannten **Zielobjekte** des **Informationsverbundes** (auch Geltungsbereich genannt). In dieser Analyse werden die **Prozesse, Anwendungen, Systeme und Geräte, Kommunikationsverbindungen**, der **Netzplan** sowie **Räume und Gebäude** (sogenannte Zielobjekte) des Geltungsbereichs erfasst.

Die Strukturanalyse bündelt all diese Informationen in einem Dokument und stellt eine **Erstaufnahme** etwa in einem Amt oder Fachbereich dar.

Voraussetzungen:

Festgelegter Geltungsbereich
(Der Geltungsbereich ist ein klar definierter und abgegrenzter Bereich, der mithilfe eines Sicherheitskonzeptes abgesichert werden soll (bspw. ein ganzes Amt oder nur ein Fachbereich oder eine einzelne Software)).

Ergebnisse

Durch die Strukturanalyse sind die Prozesse, Anwendungen, Systeme und Geräte, Räume und Gebäude, Kommunikationsverbindungen sowie ein **Netzplan** für den **Geltungsbereich** aufgenommen und **dokumentiert**.

Der **Geltungsbereich** ist schriftlich und grafisch **abgebildet**.

Was ist eine Strukturanalyse und wie wird sie durchgeführt? (2/2)

Strukturanalyse	Modellierung	IT-Grundschutz-check	Umsetzungs-planung	Sicherheitskonzept zusammenfügen

Durchführung:

1. Sicherheitsrelevante **Geschäftsprozesse** für den Geltungsbereich in einer Liste zusammentragen (Nummerierung, Name, Beschreibung, Prozessart, verarbeitete Informationen, Verantwortliche, Nutzende)
2. Verwendete **Anwendungen** sowie selbst betriebene Anwendungen des Geltungsbereichs in einer Liste sammeln (Nummerierung, Name, Beschreibung, Art, Status (in Betrieb / ruhend), Verantwortliche, Nutzende)
3. Mithilfe einer **Kreuzreferenztabelle** die Geschäftsprozesse mit den Anwendungen verknüpfen (Für welchen Geschäftsprozess brauche ich welche Anwendung?)
4. **Systeme und Geräte** des Geltungsbereichs in einer Liste sammeln (Kategorie des Gerätes, Bezeichnung, Name, Beschreibung, Plattform, Anzahl, Verantwortliche, Nutzende)
5. Mithilfe einer **Kreuzreferenztabelle** die Anwendungen mit den Systemen verknüpfen (Für welche Anwendung brauche ich welche Systeme?).
6. **Räume und Gebäude** des Geltungsbereichs identifizieren und in einer Liste dokumentieren (Nummerierung, Name, Beschreibung, Art, Anzahl, Nutzende)
7. **Kommunikationsverbindungen** (kein Muss!) herausarbeiten und in einer Liste dokumentieren (Nummerierung, Name, Beschreibung, Raum/Art, Status (in Betrieb / ruhend) Verantwortliche, Nutzende) und einen **grafischen Netzplan** erstellen, der den Geltungsbereich abbildet

Was ist eine Modellierung und wie wird sie durchgeführt? (1/2)

Strukturanalyse	**Modellierung**	IT-Grundschutz-check	Umsetzungs-planung	Sicherheitskonzept zusammenfügen

Definition:

Die Modellierung stellt grundsätzlich einen **Auswahlprozess** dar und fußt auf der Strukturanalyse.

Mithilfe der Modellierung wird der betrachtete **Informationsverbund** mittels der **IT-Grundschutz-bausteine** des Bundesamtes für Sicherheit in der Informationstechnik (BSI) **abgebildet**.

Es werden also die **relevanten Bausteine** – und damit die relevanten IT-Grundschutzchecks – für den **Geltungsbereich ausgewählt**.

Voraussetzungen:

Durchgeführte **Strukturanalyse mit** Prozessen, Anwendungen, Systemen und Geräten, Kommunikationsverbindungen und **Netzplan** sowie Räume und Gebäude (Zielobjekte) des Geltungsbereichs

Ergebnisse

Durch die Modellierung sind die **relevanten IT-Grundschutzchecks** für den Geltungsbereich **identifiziert und abgebildet.**

Was ist eine Modellierung und wie wird sie durchgeführt? (2/2)

Strukturanalyse	**Modellierung**	IT-Grundschutz-check	Umsetzungs-planung	Sicherheitskonzept zusammenfügen

Durchführung:

1. **Überblick** über die vom BSI definierten **Schichten** und dazu bereitgestellten **IT-Grundschutzbausteine** verschaffen (online auf der Webseite des BSI abrufbar)
2. Anschließend eine **Tabelle** mit den jeweiligen IT-Grundschutzbausteinen erstellen
3. Aufgrund der Strukturanalyse für jeden IT-Grundschutzbaustein **entscheiden**, ob dieser **relevant** ist **oder nicht**, und die Entscheidung kurz **dokumentiert begründen**.

   → Zur Entscheidungshilfe für die Bewertung sollten die PDF-Dateien des BSI zu den IT-Grundschutzbausteinen danebengelegt werden. In diesen Dateien wird genau beschrieben, wann welcher IT-Grundschutzbaustein relevant ist und welche aufgrund der getroffenen Entscheidung gegebenenfalls ebenfalls relevant werden.

Was ist der IT-Grundschutzcheck und wie wird er durchgeführt? (1/2)

Strukturanalyse	Modellierung	**IT-Grundschutz-check**	Umsetzungs-planung	Sicherheitskonzept zusammenfügen

Definition:

Der **IT-Grundschutzcheck fußt** auf der **Modellierung** und dient dazu, **Schwachstellen** und **Sicherheitslücken aufzudecken**.

Beim IT-Grundschutzcheck werden **Anforderungen** an das entsprechende **Sicherheitsniveau** der Institution auf ihre Umsetzung hin **geprüft**.

Voraussetzungen:

Durchgeführte **Strukturanalyse mit Netzplan** zum Geltungsbereich und relevante **IT-Grundschutzchecks** sind identifiziert.

Ergebnisse

Durch den IT-Grundschutzcheck sind nicht oder nur teilweise umgesetzte sicherheitsrelevante Anforderungen sichtbar, wodurch **(potenzielle) Sicherheitslücken und Einfallstore offenkundig** werden.

Was ist der IT-Grundschutzcheck und wie wird er durchgeführt? (2/2)

Strukturanalyse	Modellierung	**IT-Grundschutz-check**	Umsetzungs-planung	Sicherheitskonzept zusammenfügen

Durchführung:

1. Auf Grundlage der Modellierung die **relevanten IT-Grundschutzchecks des BSI beschaffen** (online auf der Webseite des BSI abrufbar)
2. Möglichen **Personenkreis** für das Ausfüllen der IT-Grundschutzchecks entsprechend der Themen benennen (bspw. für die IT-Grundschutzchecks im Bereich Betrieb und IT-Systeme IT-ler:innen kontaktieren oder für den Bereich Personal und Organisation eine Verwaltungsfachkraft benennen)
3. Die Anforderungen in den IT-Grundschutzchecks entsprechend der zu erreichenden Sicherheitsstufe (Basis-Absicherung, Standard-Absicherung, Hoher Schutzbedarf) filtern
4. Die IT-Grundschutzchecks bearbeiten und die **Anforderungen** Schritt für Schritt **beantworten** - wichtig ist hierbei die **Begründung** für die **Umsetzung/Nicht-Umsetzung**: Je besser etwa Ablageorte / geregelte Anweisungen dokumentiert sind, desto leichter lassen sich diese bei einer Testierung oder Zertifizierung von einem/einer Auditor:in wiederfinden
5. Nicht umgesetzte Anforderungen für die spätere Umsetzungsplanung **farblich** hervorheben

Was ist die Umsetzungsplanung und wie wird sie durchgeführt? (1/2)

Strukturanalyse	Modellierung	IT-Grundschutz-check	**Umsetzungs-planung**	Sicherheitskonzept zusammenfügen

Definition:

Die **Umsetzungsplanung fußt** auf der Bearbeitung der für den Geltungsbereich relevanten **IT-Grundschutzchecks**.

Für die dort sichtbar gewordenen, **nicht oder nur teilweise umgesetzten Anforderungen** müssen nun **Maßnahmen entwickelt** werden.

Voraussetzungen:

Durchgeführte **Strukturanalyse** mit **Netzplan** und **Modellierung** sowie ausgefüllte **IT-Grundschutzchecks.**

Ergebnisse

Abgeleitete **Maßnahmen** mit konkreten **Zuständigkeiten und Verantwortlichkeiten**, die in einer **Zeitplanung für die Umsetzung** der Maßnahmen münden.

Was ist die Umsetzungsplanung und wie wird sie durchgeführt? (2/2)

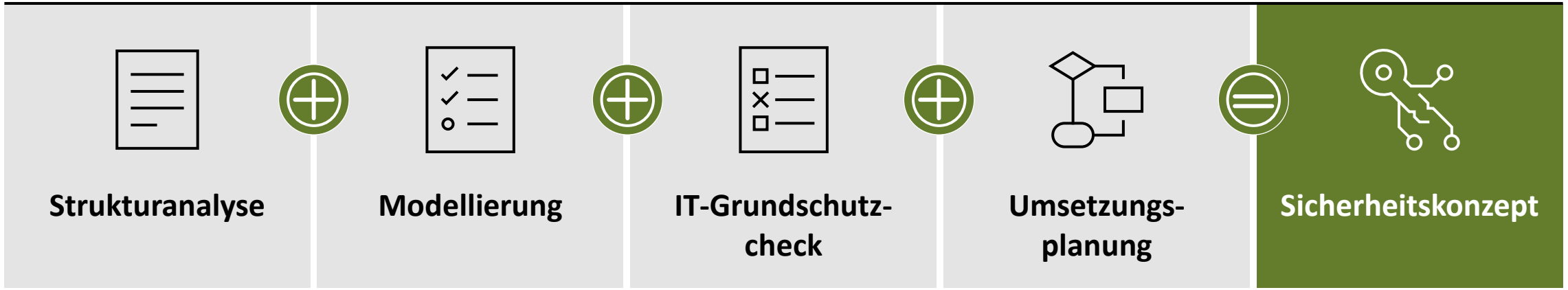
Strukturanalyse	Modellierung	IT-Grundschutz-check	**Umsetzungs-planung**	Sicherheitskonzept zusammenfügen

Durchführung:

1. Eine **Tabelle** mit den **nicht oder nur teilweise umgesetzten Anforderungen** für den Geltungsbereich erstellen (Schicht, Baustein, Nummerierung der Maßnahme, Konkretisierung der Anforderung (aus IT-Grundschutzcheck zu entnehmen bspw. A1, A2, A3, A11, A15), empfohlene Umsetzungsreihenfolge des BSI (R1, R2, R3), Anforderung, Maßnahme, Ist-Stand, Zuständigkeit für die Umsetzung, Beginn der Maßnahme, Status, Verschlagwortung)
2. In mehreren **Workshops** gemeinsam mit den notwendigen **Akteuren** die Maßnahmen ableiten und in der Tabelle vermerken
3. Anschließend **Zuständigkeiten** und **Verantwortlichkeiten** (rollenspezifisch – nicht personenspezifisch!) benennen
4. Einschätzung zum kurz-, mittel- oder langfristigen **Beginn der Maßnahme** abgeben
5. **Status** zu jeder Maßnahme festhalten (Umsetzung ausstehend, Umsetzung begonnen, Umsetzung abgeschlossen)
6. Für die einfachere und gebündelte Abarbeitung der Maßnahmen kann jede mit einem **Schlagwort** versehen werden (wenn dann bspw. eine Dienstanweisung (DA) aufgrund unterschiedlicher Anforderungen in unterschiedlichen IT-Grundschutzchecks angepasst werden muss, kann nach diesem Schlagwort gefiltert und alle Anforderungen in die neue Version einer DA eingearbeitet werden)

Durch diese zuvor erstellten Unterlagen entsteht Ihr Sicherheitskonzept nach BSI-Standard auf dem Niveau einer Basis-Absicherung.

Das Sicherheitskonzept ergibt sich aus den Unterlagen, die in den zuvor genannten Schritten erstellt wurden.



Flankierend zum Sicherheitskonzept muss eine **Leitlinie für Informationssicherheit** verabschiedet werden. Diese enthält den Geltungsbereich, Zwecke und Ziele, Sicherheitsziele für die Institution, die Aufbau- und Organisationsstruktur in Bezug auf die Informationssicherheit sowie Schlussbestimmungen (Verpflichtungen, Bekanntgabe, Zuwiderhandlungen und Folgen).

Kontakt

Uta Fiedler
Managerin
Standort Hamburg
M +49 1722614501
Uta.Fiedler@pd-g.de

Nesrin Tanrikulu
Consultant
Standort Berlin
M +49 172 2197817
Nesrin.Tanrikulu@pd-g.de

Daniel Göttl
Consultant
Standort Hamburg
M +49 173 593 32 64
Daniel.Goettl@pd-g.de

info@pd-g.de
www.pd-g.de

PD – Berater der öffentlichen Hand GmbH
Friedrichstraße 149, 10117 Berlin
T +49 30 25 76 79 - 0
F +49 30 25 76 79 - 199

Diese Präsentation ist Eigentum der PD – Berater der öffentlichen Hand GmbH.
Jede Verwertung, Weitergabe oder Verwendung der Präsentation ohne Zustimmung ist unzulässig.
© 2026 PD – Berater der öffentlichen Hand GmbH

Hidden Champion
2026/27

PD – Berater der öffentlichen Hand GmbH
Friedrichstraße 149, 10117 Berlin
T +49 30 25 76 79 - 0
F +49 30 25 76 79 - 199

info@pd-g.de
www.pd-g.de

Hidden Champion
2026/27

Diese Präsentation ist Eigentum der PD – Berater der öffentlichen Hand GmbH.
Jede Verwertung, Weitergabe oder Verwendung ohne Zustimmung ist unzulässig.
© 2026 PD – Berater der öffentlichen Hand GmbH