DEUTSCHER
LANDKREISTAG

# Ein kurzer Überblick über Vorgehensweisen und Profile im IT-Grundschutz des BSI

Der IT-Grundschutz des BSI besteht aus den **BSI-Standards** und dem **IT-Grundschutz-Kompendium**. Die BSI-Standards enthalten Methoden und Vorgehensweisen zu den unterschiedlichsten Themen aus dem Bereich der Informationssicherheit.

- Der **BSI-Standard 200-1** definiert allgemeine **Anforderungen an ein Managementsystem für Informationssicherheit (ISMS)**.
- Mit dem **BSI-Standard 200-2** zur **IT-Grundschutz-Methodik** kann ein solides ISMS aufgebaut werden. Dabei steht mit der Standard-Absicherung die bewährte IT-Grundschutz-Vorgehensweise zur Verfügung. Sie wird ergänzt durch die Basis-Absicherung, die eine grundlegende Erst-Absicherung in der Breite ermöglicht, sowie durch die Kern-Absicherung, die sich dem Schutz der besonders schützenswerten Daten („Kronjuwelen“) einer Institution widmet.
- Der **BSI-Standard 200-3** zum **Risikomanagement** enthält alle risikobezogenen Arbeitsschritte bei der Umsetzung des IT-Grundschutzes.
- Der **BSI-Standard 100-4** befasst sich mit dem **Notfallmanagement**. Er wird derzeit grundlegend überarbeitet und soll 2020 als **BSI-Standard 200-4 „Business Continuity Management“ (BCM)** veröffentlicht werden.

## Schutzbedarfsfeststellung nach BSI-Standard 200-2

(Für die Schutzziele „Vertraulichkeit", „Integrität" und „Verfügbarkeit" gesondert anzuwenden.)

| Schutzbedarfs-kategorien / Schadensszenarien | "normal"<br>*Die Schadensauswirkungen sind begrenzt und überschaubar.* | "hoch"<br>*Die Schadensauswirkungen können beträchtlich sein.* | "sehr hoch"<br>*Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.* |
|---|---|---|---|
| 1. Verstoß gegen Gesetze / Vorschriften / Verträge | • Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen<br>• Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen | • Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen<br>• Vertragsverletzungen mit hohen Konventionalstrafen | • Fundamentaler Verstoß gegen Vorschriften und Gesetze<br>• Vertragsverletzungen, deren Haftungsschäden ruinös sind |
| 2. Beeinträchtigung des informationellen Selbstbestimmungsrechts | • Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann. | • Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen<br>• Vertragsverletzungen mit hohen Konventionalstrafen | • Es handelt sich um personenbezogene Daten, bei deren Verarbeitung eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen gegeben ist. |
| 3. Beeinträchtigung der persönlichen Unversehrtheit | • Eine Beeinträchtigung erscheint nicht möglich | • Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden. | • Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich.<br>• Gefahr für Leib und Leben |
| 4. Beeinträchtigung der Aufgabenerfüllung | • Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden.<br>• Die maximal tolerierbare Ausfallzeit liegt zwischen 24 und 72 Stunden. | • Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt.<br>• Die maximal tolerierbare Ausfallzeit liegt zwischen einer und 24 Stunden. | • Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden.<br>• Die maximal tolerierbare Ausfallzeit ist kleiner als eine Stunde. |
| 5. Negative Innen- oder Außenwirkung | • Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten. | • Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten. | • Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, eventuell sogar existenzgefährdender Art, ist denkbar. |
| 6. Finanzielle Auswirkungen | • Der finanzielle Schaden bleibt für die Institution tolerabel. | • Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend. | • Der finanzielle Schaden ist für die Institution existenzbedrohend. |

- Die Vererbung der Schutzbedarfe erfolgt nach den Vererbungsprinzipien: Maximumprinzip, Kummulationsprinzip, Verteilungsprinzip.

- Relevante BSI-Standards:
  - BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)
  - BSI-Standard 200-2: IT-Grundschutz-Methodik
  - BSI-Standard 200-3: Risikomanagement
  - BSI-Standard 100-4: Notfallmanagement

*[Zusammenfassung: Heino Sauerbrey (DLT) auf Basis des BSI-Standards 200-2]*

Das **Grundschutz-Kompendium** besteht aus den Kapiteln

- Elementare Gefährdungen
- Bausteine
- Umsetzungshinweise
- Anleitung zur Migration

Die **Bausteine** sind in zehn Schichten aufgeteilt

- ISMS: Sicherheitsmanagement
- ORP: Organisation und Personal
- CON: Konzeption und Vorgehensweise
- OPS: Betrieb
- DER: Detektion und Reaktion
- APP: Anwendungen
- SYS: IT-Systeme
- IND: Industrielle IT
- NET: Netze und Kommunikation
- INF: Infrastruktur

**Grundschutz-Profile** sind **Muster-Sicherheitskonzepte für abgegrenzte Anwendungsbereiche.**
Sie werden durch Vertreter einer „Branche“ unter Einbeziehung des BSI für die betreffende Branche erarbeitet.
Eine Arbeitsgruppe der Bundesvereinigung der kommunalen Spitzenverbände hat mit dem IT-Grundschutzprofil „Basis-Absicherung Kommunalverwaltung“ („Kommunalprofil“) das erste Branchenprofil des modernisierten IT-Grundschutzes erarbeitet und bereits einmal aktualisiert.
Das Profil kann unter http://down.it-sibe-forum.de/ heruntergeladen werden.

Aktuell arbeitet eine weitere Arbeitsgruppe der BV an einem „Schulprofil“


IT-GRUNDSCHUTZ-PROFIL

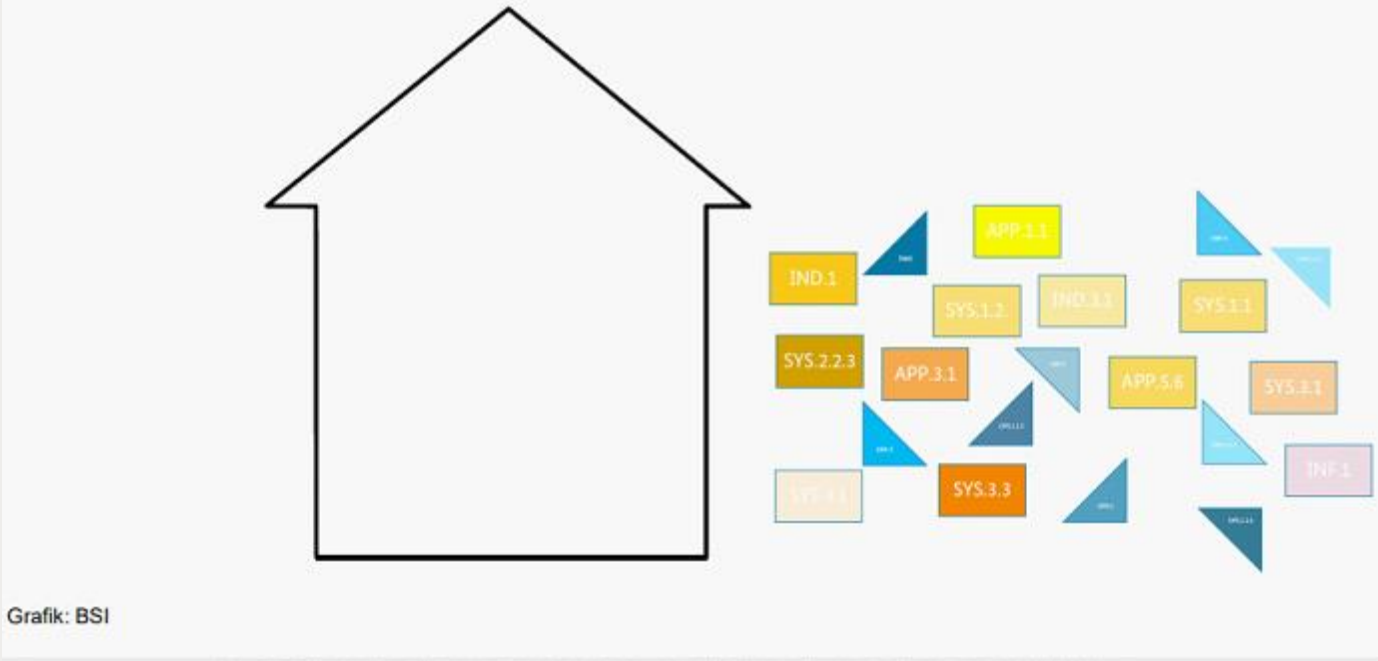
BASIS-ABSICHERUNG KOMMUNALVERWALTUNG

Version 2.0
15.10.2019

Deutscher Städtetag · DEUTSCHER LANDKREISTAG · DStGB

ARBEITSGRUPPE „MODERNISIERUNG IT-GRUNDSCHUTZ“ mit Unterstützung durch
Deutscher Städtetag
Deutscher Landkreistag
Deutscher Städte- und Gemeindebund

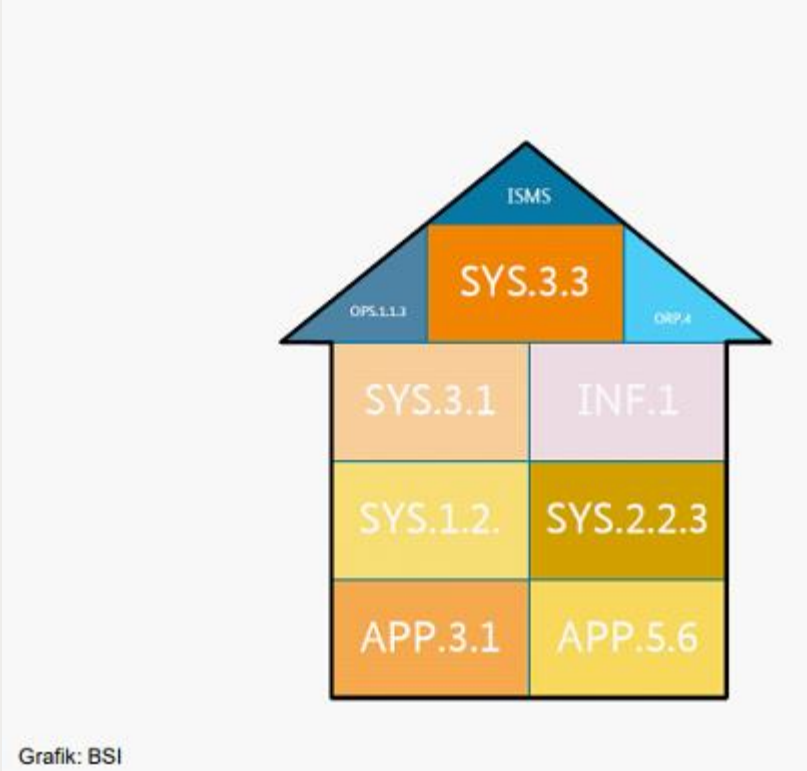
**Grundschutz-Profile** sind Muster-Sicherheitskonzepte für abgegrenzte Anwendungsbereiche.
Sie werden durch Vertreter einer „Branche“ unter Einbeziehung des BSI für die betreffende Branche erarbeitet.




Grafik: BSI

**Grundschutz-Bausteine:**
ISMS: Sicherheitsmanagement
ORP: Organisation und Personal
CON: Konzeption und Vorgehensweise
OPS: Betrieb
DER: Detektion und Reaktion
APP: Anwendungen
SYS: IT-Systeme
IND: Industrielle IT
NET: Netze und Kommunikation
INF: Infrastruktur

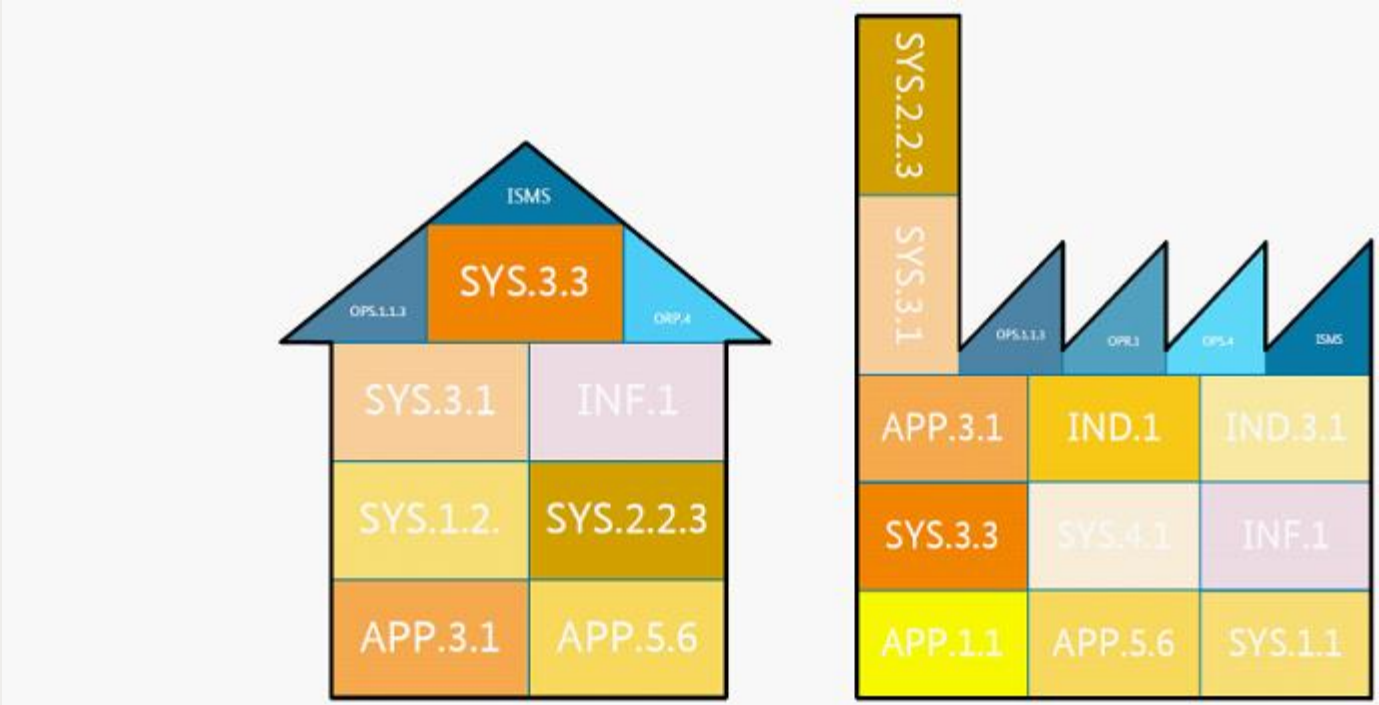
**Grundschutz-Profile** sind Muster-Sicherheitskonzepte für abgegrenzte Anwendungsbereiche.
Sie werden durch Vertreter einer „Branche“ unter Einbeziehung des BSI für die betreffende Branche erarbeitet.




Grafik: BSI

**Grundschutz-Bausteine:**
ISMS: Sicherheitsmanagement
ORP: Organisation und Personal
CON: Konzeption und Vorgehensweise
OPS: Betrieb
DER: Detektion und Reaktion
APP: Anwendungen
SYS: IT-Systeme
IND: Industrielle IT
NET: Netze und Kommunikation
INF: Infrastruktur

**Grundschutz-Profile** sind Muster-Sicherheitskonzepte für abgegrenzte Anwendungsbereiche.
Sie werden durch Vertreter einer „Branche“ unter Einbeziehung des BSI für die betreffende Branche erarbeitet.




Grafik: BSI

**Grundschutz-Bausteine:**
ISMS: Sicherheitsmanagement
ORP: Organisation und Personal
CON: Konzeption und Vorgehensweise
OPS: Betrieb
DER: Detektion und Reaktion
APP: Anwendungen
SYS: IT-Systeme
IND: Industrielle IT
NET: Netze und Kommunikation
INF: Infrastruktur

# IT-Grundschutz

## ORP.2 Personal

**Schnell zum Abschnitt**



### IT-Grundschutz-Kompendium

# 2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein ORP.2 *Personal* von besonderer Bedeutung:

## 2 1 Personalausfall

Der Ausfall von Personal kann dazu führen, dass bestimmte Aufgaben nicht mehr oder nicht zeitnah wahrgenommen werden können.

## 2 2 Missbrauch von Berechtigungen

Jeder, der Informationen bearbeiten soll, benötigt dafür angemessene Berechtigungen. Nutzer können diese missbrauchen, indem sie diese ausnutzen, um Informationen zu manipulieren, weiterzugeben oder auf andere Weise der Institution zu schaden.

## 2 3 Fehlende oder unzureichende Regelungen

Wenn Regelungen zur Informationssicherheit fehlen, unzureichend, nicht umsetzbar oder unverständlich sind, kann das dazu führen, dass notwendige Sicherheitsmaßnahmen nicht umgesetzt werden (siehe auch G 0.29 *Verstoß gegen Gesetze oder Regelungen*).

## 2 4 Unzureichende Kenntnis über Regelungen

Die Festlegung von Regelungen allein sichert noch nicht deren Beachtung und keinen störungsfreien Betrieb. Allen Mitarbeitern müssen die geltenden Regelungen auch bekannt sein, vor allem den Funktionsträgern. Ein Schaden, der entsteht, weil bestehende Regelungen nicht bekannt sind, darf sich

## 3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein Personal vorrangig umgesetzt werden:

### ORP.2.A1 Geregelte Einarbeitung neuer Mitarbeiter [Vorgesetzte]

Die Personalabteilung sowie die Vorgesetzten MÜSSEN dafür sorgen, dass neue Mitarbeiter zu Beginn ihrer Beschäftigung in ihre neuen Aufgaben eingearbeitet und über bestehende Regelungen, Gepflogenheiten und Verfahrensweisen informiert werden. Hierbei SOLLTE eine Checkliste unterstützend wirken.

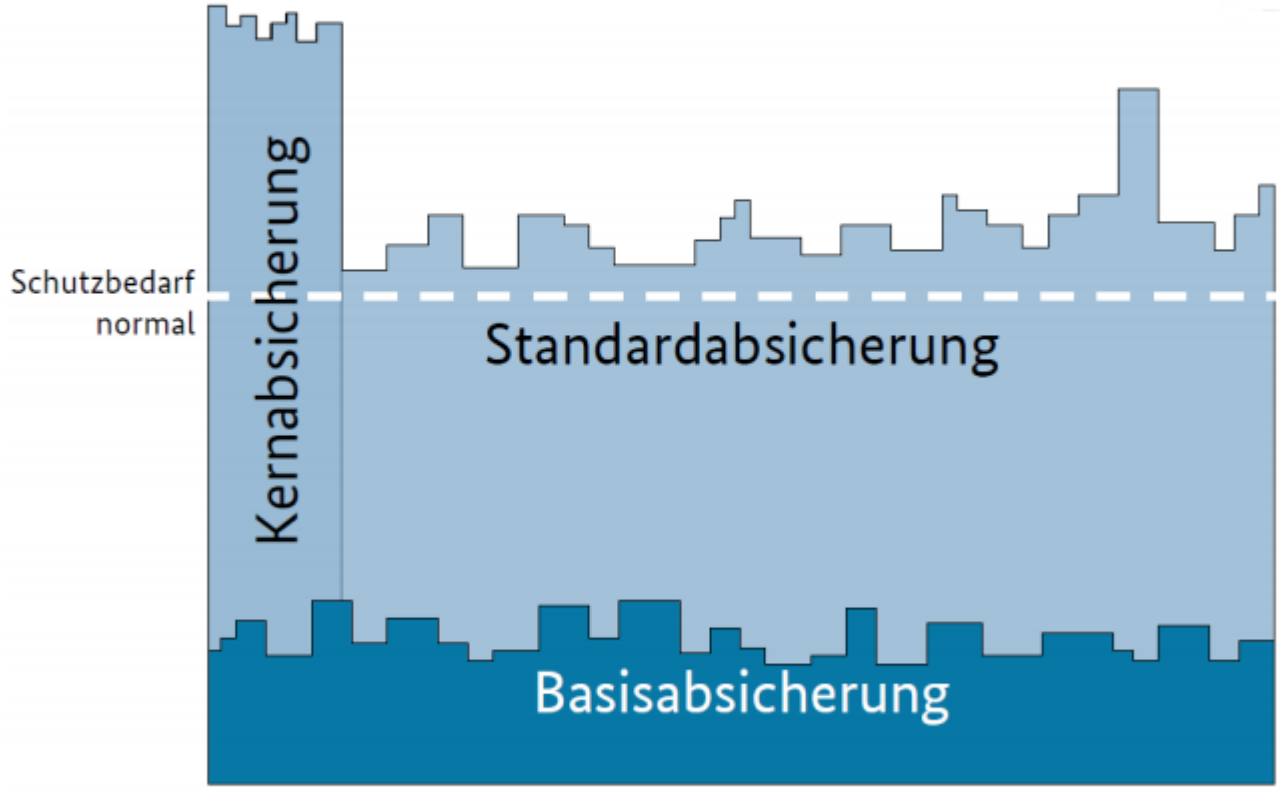
Zur geregelten Einarbeitung neuer Mitarbeiter MÜSSEN diese auf bestehende Regelungen und Handlungsanweisungen zur Informationssicherheit hingewiesen werden. Alle Mitarbeiter MÜSSEN über Regelungen zur Informationssicherheit, deren Veränderungen und ihre spezifischen Auswirkungen auf einen Geschäftsprozess oder auf das jeweilige Arbeitsumfeld unterrichtet werden.

Alle Mitarbeiter MÜSSEN explizit darauf verpflichtet werden, einschlägige Gesetze, Vorschriften und interne Regelungen einzuhalten. Außerdem MÜSSEN alle Mitarbeiter darauf hingewiesen werden, dass alle während der Arbeit erhaltenen Informationen ausschließlich zum internen Gebrauch bestimmt sind, solange sie nicht anders gekennzeichnet sind.

### ORP.2.A2 Geregelte Verfahrensweise beim Weggang von Mitarbeitern [Vorgesetzte, IT-Betrieb]

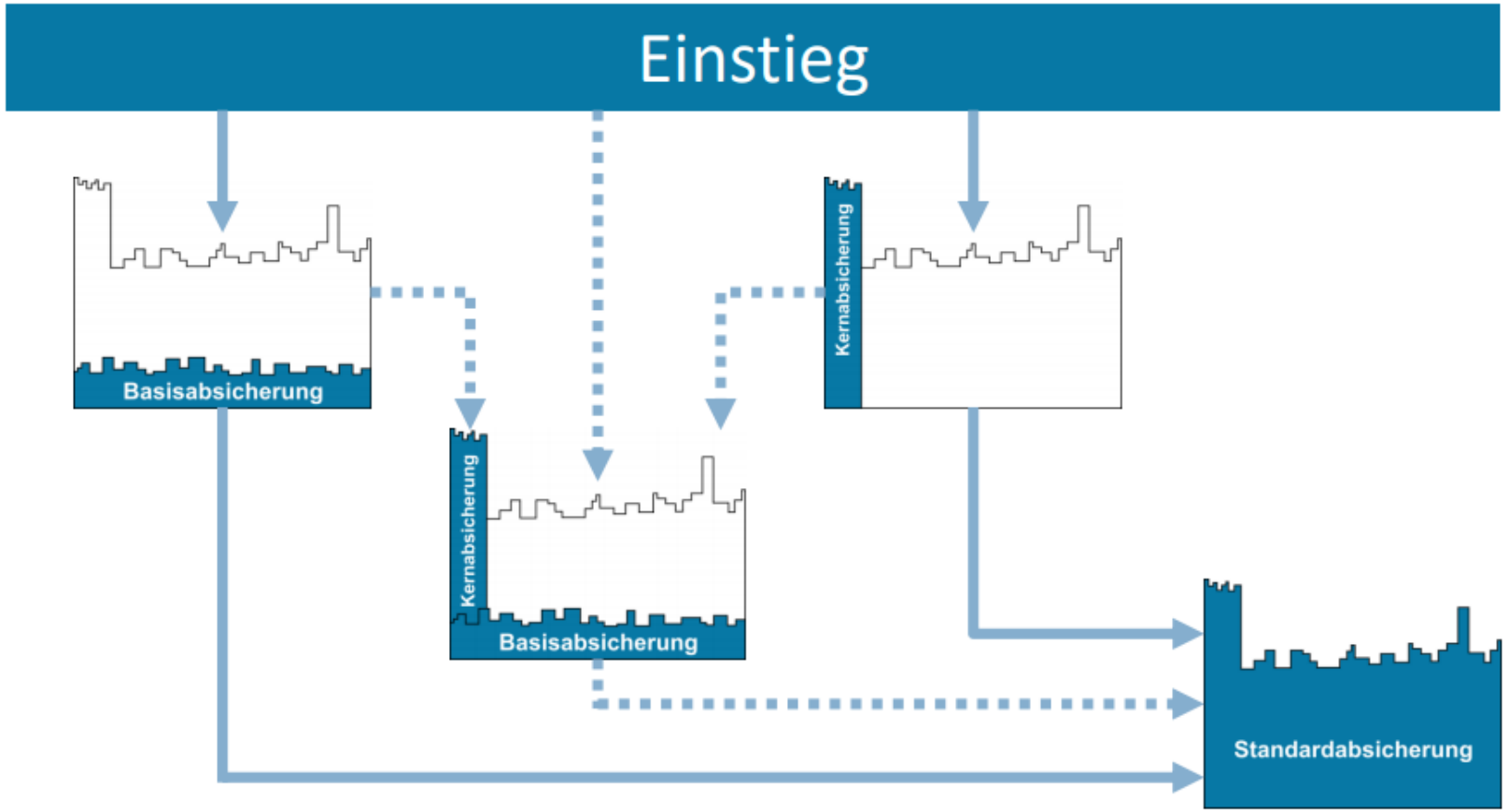
Vor dem Weggang eines Mitarbeiters MUSS eine rechtzeitige Einweisung des Nachfolgers, idealerweise durch den ausscheidenden Mitarbeiter, durchgeführt werden. Ist eine direkte Übergabe nicht möglich, MUSS vom ausscheidenden Mitarbeiter eine ausführliche Dokumentation angefertigt werden. Außerdem MÜSSEN von ausscheidenden Mitarbeitern alle im Rahmen ihrer Tätigkeit erhaltenen Unterlagen, Schlüssel und Geräte sowie Ausweise und Zutrittsberechtigungen

# Vorgehensweisen




Grafik: BSI

# Wege zur Standardabsicherung
## IT-Grundschutz

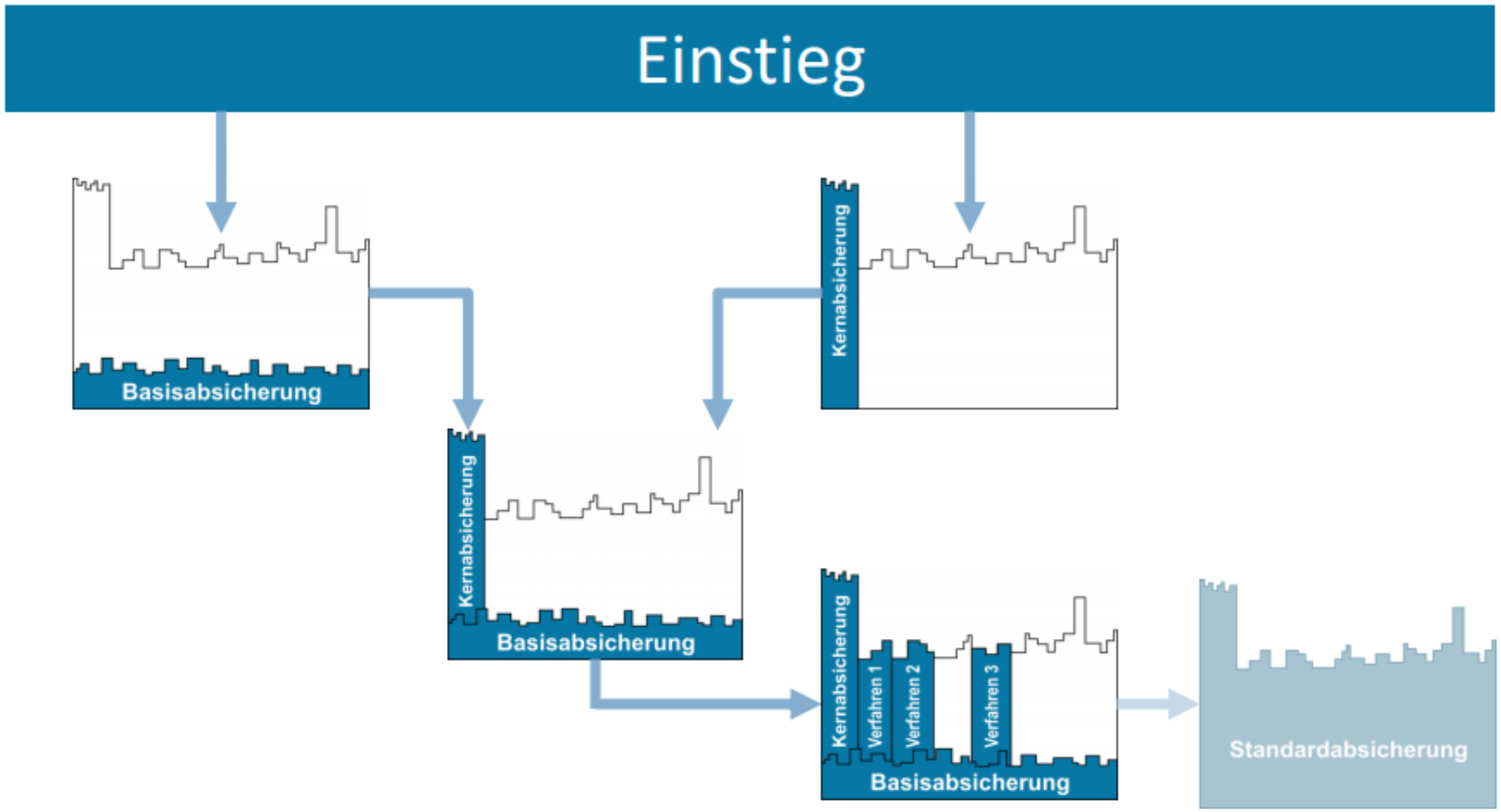



Grafik: BSI

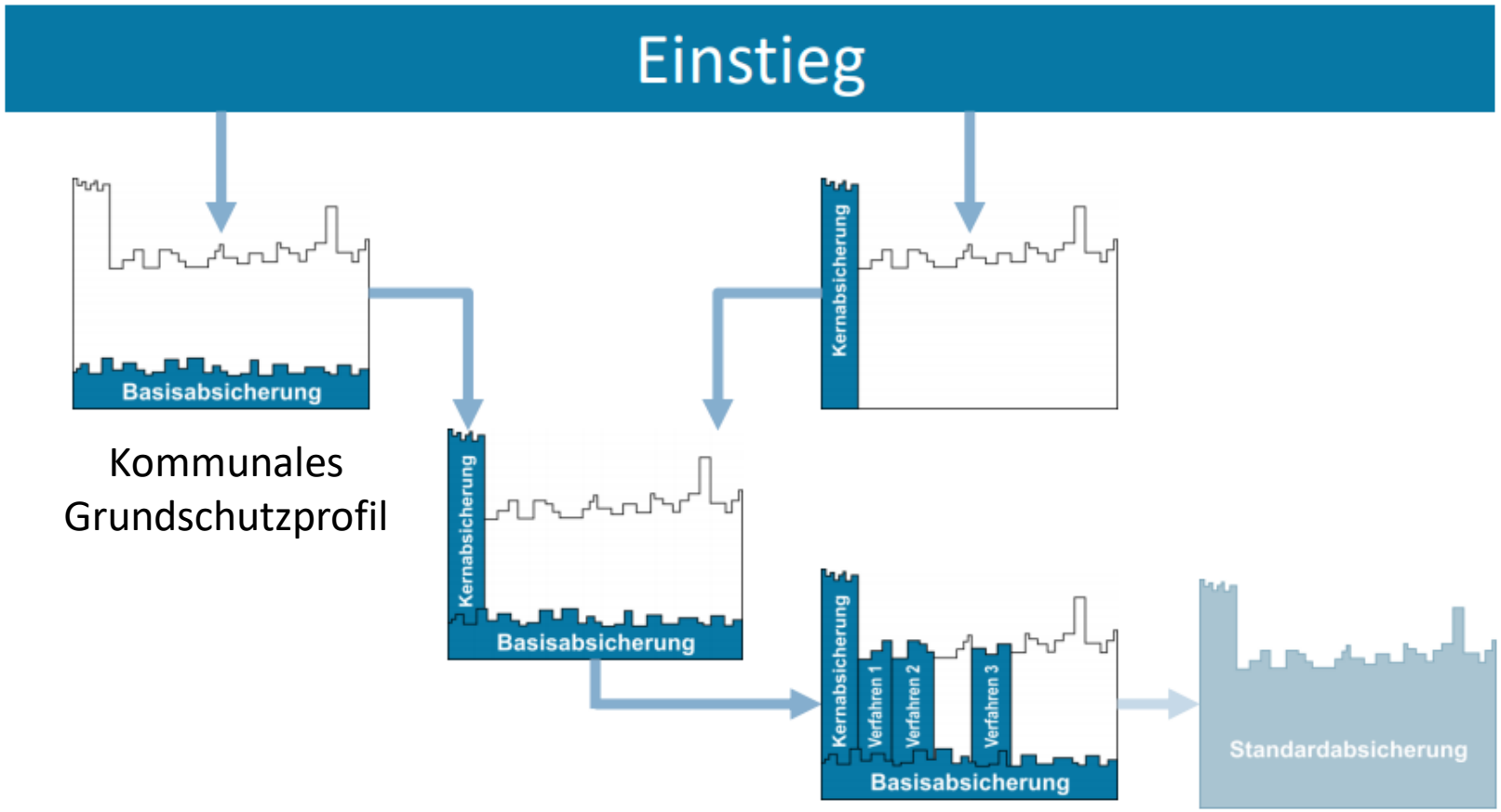
13 IT-Grundschutz im kommunalen Profil • Personal- und Organisationsamt • Jens Lange • 12.09.2017

# Wege zur Standardabsicherung

## „Kasseler Modell“



# Wege zur Standardabsicherung
## „Kasseler Modell“




Kernabsicherung
Verfahren 1
Verfahren 2
Verfahren 3
Basisabsicherung


Nationales Waffenregister
EU-Zahlstelle
Verbindungsnetz
i-Kfz MSADP
Basisabsicherung


Nationales Waffenregister
EU-Zahlstelle
GS-Profil
VN TNA
Verbindungsnetz
GS-Profil
i-Kfz MSADP
Basisabsicherung


Nationales Waffenregister
EU-Zahlstelle
GS-Profil
VN TNA
Verbindungsnetz
GS-Profil
i-Kfz MSADP
GS-Profil Wahl?
Basisabsicherung