

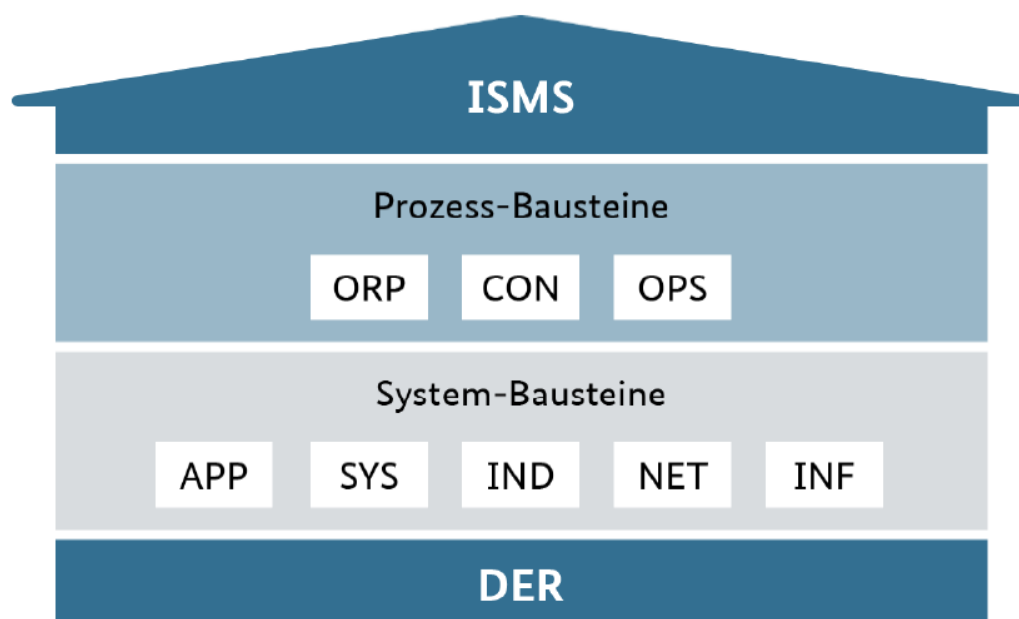


Die IT-Grundschatz Bausteine



Das IT-Grundschatz-Kompodium ist **modular** aufgebaut. Den Kern bilden die **IT-Grundschatz-Bausteine**, in denen jeweils für einen bestimmten Aspekt der Informationssicherheit **typische Gefährdungen und Sicherheitsanforderungen** beschrieben werden. Gegenstand eines Bausteins können übergeordnete Themen sein wie das Informationssicherheits- oder Notfallmanagement, aber auch mehr oder weniger spezielle technische Systeme, die üblicherweise in Unternehmen und Behörden im Einsatz sind, etwa Clients und Server, mobile Systeme oder auch industrielle Steuerungen.

Die verschiedenen IT-Grundschatz-Bausteine sind in ein Schichtenmodell gegliedert, das wie folgt aussieht:



Die vorgenommene Einteilung der Bausteine bietet eine Reihe von Vorteilen. So wird durch die vorgenommene Aufteilung die Komplexität dieses Themas zweckmäßig reduziert und Redundanzen werden vermieden. Dies erleichtert es auch, gezielt Einzelaspekte eines entwickelten Sicherheitskonzepts zu aktualisieren, ohne dass davon andere Teile des Konzepts beeinflusst werden.

Die einzelnen Schichten sind darüber hinaus so gewählt, dass Zuständigkeiten gebündelt sind. So adressieren die Schichten ISMS und ORP primär das Sicherheitsmanagement einer Institution, die Schicht INF die Haustechnik und die Schichten SYS, NET und APP die für IT-Systeme, Netze und Anwendungen jeweils zuständigen Verantwortlichen, Administratoren und Betreiber.

Die im Schichtenmodell vorhandenen Bausteine sind immer in gleicher Weise aufgebaut:

- Sie beginnen mit einer **kurzen Beschreibung** und Abgrenzung des behandelten Sachverhalts.
- Es folgt eine Darstellung der spezifischen **Gefährdungslage** mit Hilfe exemplarischer Gefährdungen.
- Den Kern bilden die in drei Gruppen unterteilten **Sicherheitsanforderungen**:
 - vorrangig zu erfüllende **Basis-Anforderungen**,
 - für eine vollständige Umsetzung des IT-Grundschutzes und eine dem Stand der Technik gemäße Sicherheit zusätzlich zu erfüllende **Standard-Anforderungen** sowie
 - Anforderungen für den **erhöhten Schutzbedarf**.
- Den Abschluss bilden **Verweise** auf weiterführende Informationen sowie eine **Kreuzreferenztable**, in der die Anforderungen mit den jeweils zutreffenden elementaren Gefährdungen miteinander in Bezug gesetzt werden.

Die Anforderungen beschreiben, was getan werden **MUSS** oder **SOLLTE**. In Großbuchstaben gesetzte Verben zeigen dabei die **Verbindlichkeit einer Anforderung**. Die nachfolgende Tabelle gibt hierzu eine Übersicht:

Ausdruck	Bedeutung
MUSS, DARF NUR	So gekennzeichnete Anforderungen müssen unbedingt erfüllt werden.
DARF NICHT, DARF KEIN	Etwas darf in keinem Fall getan werden.
SOLLTE	Dieser Ausdruck bedeutet, dass eine Anforderung zwar normalerweise erfüllt werden muss, bei stichhaltigen Gründen aber auch davon abgesehen werden kann.
SOLLTE NICHT, SOLLTE KEIN	Dieser Ausdruck bedeutet, dass etwas normalerweise nicht getan werden darf, bei stichhaltigen Gründen aber trotzdem erfolgen kann.



Aufgabenstellung:

Beantworten Sie folgende Fragen!

Nennen Sie den Kern des IT-Grundschutz-Kompodiums!

IT-Grundschutz-Bausteine

Welche Aspekte werden darin beschrieben?

Typische Gefährdungen und Sicherheitsanforderungen

z.B. Informationssicherheitsmanagement bzw. Notfallmanagement oder spezielle technische Systeme

In welche Kategorien werden die Bausteine im Schichtenmodell aufgeteilt?

Prozessbausteine

Systembausteine

Nennen Sie die Vorteile des Schichtenmodells!

Komplexität wird Reduziert

Redundanzen werden vermieden -> einzelaspekte können problemlos aktualisiert werden

Zuständigkeiten sind gebündelt (Schichten adressieren jeweils Verantwortliche, Admins und Betreiber)

Beschreiben Sie den Aufbau der IT-Grundschutz Bausteine!

Immer gleicher Aufbau:

Kurze Beschreibung und Abgrenzung

Darstellung der Gefährdungslage

Sicherheitsanforderungen

Verweise und Kreuzreferenztafel

Nennen Sie die drei Gruppen, in die die Sicherheitsanforderungen unterteilt werden!

Basis Anforderungen

Standard Anforderungen

Anforderungen für erhöhten Schutzbedarf

Wie werden die Verbindlichkeiten der Anforderungen dargestellt?

Muss/Darf nur

Darf nicht/Darf kein

Sollte

Sollte nicht/Sollte kein