

# IT-Grundschutz-Profil für die Nutzung der E-Akte Bund

Version:	1.0
Revisionszyklus:	2 Jahre
Edition IT-Grundschutz-Kompendium:	2023

# Inhaltsverzeichnis

1	Einleitung.....	4
2	Formale Aspekte.....	5
3	Haftungsausschluss .....	6
4	Liste der Autorinnen und Autoren.....	7
5	Management Summary.....	8
5.1	Zielgruppe.....	8
5.2	Zielsetzung.....	8
5.3	Abdeckung Vorgehensweise.....	8
5.4	ISO 27001-Kompatibilität.....	8
5.5	Aufgaben der Leitungsebene .....	8
6	Festlegung des Geltungsbereichs .....	9
6.1	Beschreibung des Schutzbedarfs.....	9
6.2	Abgrenzung des Informationsverbundes .....	9
6.2.1	Beschreibung des Musterszenarios.....	9
6.2.2	Beschreibung des Informationsverbunds .....	10
6.3	Strukturanalyse .....	11
6.3.1	Geschäftsprozesse / Fachaufgaben .....	11
6.3.2	Netzplan .....	12
6.3.3	Anwendungen.....	13
6.3.4	IT-Systeme.....	14
6.3.5	Netze und Netzkomponenten .....	15
6.3.6	Gebäude und Räume .....	15
6.4	Umgang mit Abweichungen .....	16
7	Zu erfüllende Anforderungen und umzusetzende Maßnahmen.....	17
7.1	Feststellung des Schutzbedarfs .....	17
7.2	Zuordnung der relevanten Bausteine.....	17
7.3	Relevanz der Anforderungen.....	23
8	Risikoanalyse / Restrisiko .....	24
9	Anwendungshinweise .....	25
9.1	Anwendung in vollständig konsolidierten Nutzerbehörden.....	25

9.2	Anwendung in nicht oder teilweise konsolidierten Nutzerbehörden.....	25
9.3	Hinweise zu einzelnen Bausteinen .....	25
10	Anhang .....	33
10.1	Verzeichnisse .....	33
10.1.1	Abbildungsverzeichnis .....	33
10.1.2	Tabellenverzeichnis.....	33
10.2	Mitgeltende und referenzierte Dokumente.....	33
10.3	Unterstützende Informationen .....	34
10.4	Glossar .....	34
10.5	Abkürzungen.....	37

## Versionshistorie

Datum	Version	Änderung	Bearbeiter
11.07.2024	1.0	Fertigstellung Version 1.0	Siehe Liste Autorinnen und Autoren

# 1 Einleitung

Ziel der Erstellung eines IT-Grundschutz-Profiles ist es, für bestimmte Anwendungsfelder Musterszenarien anzubieten, die es den Anwendenden aus der jeweiligen Zielgruppe erleichtern, den Sicherheitsprozess nach IT-Grundschutz auf ihre individuellen Rahmenbedingungen abzubilden. Ein IT-Grundschutz-Profil ist eine Schablone für ein ausgewähltes Szenario, mit dem die IT-Grundschutz-Umsetzung für diesen Bereich konkretisiert wird. Über ein IT-Grundschutz-Profil werden verschiedene Schritte des Informationssicherheitsprozesses für einen definierten Anwendungsbereich so aufbereitet, dass es als Rahmen für Sicherheitskonzepte adaptiert werden kann.

Die Bundesverwaltung umfasst ca. 200 Behörden mit etwa 450.000 Mitarbeitenden. Die E-Akte Bund ermöglicht die elektronische Aktenführung inklusive Dokumentenworkflow anhand eines einheitlichen Dokumentenmanagementsystems (DMS), welches allen Bundesbehörden zentral bereitgestellt wird. Die E-Akte Bund ist eine Lösung, die den ressortabgestimmten Anforderungen entspricht und es darüber hinaus ermöglicht, angrenzende Verfahren, wie bspw. Fachverfahren, über offene Standards anzubinden.

Die E-Akte Bund wird als zentraler Dienst der Bundesverwaltung in den Rechenzentren des ITZBund betrieben (Bereitstellung). Nutzerbehörden können über die Netze des Bundes (NdB) aus ihrem eigenen Hausnetz auf die E-Akte Bund zugreifen (Nutzung).

Für eine umfassende Betrachtung der Informationssicherheit der E-Akte Bund muss das Zusammenwirken der Informationssicherheit des zentralen Dienstes E-Akte Bund, der Nutzerbehörden sowie der verwendeten Netzverbindungen berücksichtigt werden.

## 2 Formale Aspekte

Aspekt	Beschreibung
Titel:	IT-Grundschutz-Profil für die Nutzung der E-Akte Bund
Ansprechpersonen:	Siehe Liste der Autorinnen und Autoren (Tabelle 2)
Herausgeber:	Anwendendengruppe
Version:	1.0
IT-Grundschutz-Kompendium:	Edition 2023
Revisionszyklus:	2 Jahre
Vertraulichkeit:	-/-

*Tabelle 1: Formale Aspekte*

### **3      Haftungsausschluss**

Dieses Dokument wurde mit größter Sorgfalt erstellt, erhebt aber keinen Anspruch auf Vollständigkeit und Richtigkeit. Die Autorinnen und Autoren haben keinen Einfluss auf die Nutzung dieses IT-Grundschutz-Profiles durch Anwenderinnen und Anwender, sodass sie naturgemäß für die Auswirkungen auf die Rechtsposition der Parteien keine Haftung übernehmen können.

## 4 Liste der Autorinnen und Autoren

Name	Organisation
Heinrich Altengarten	Bundesamt für Sicherheit in der Informationstechnik
Claudia Bode	Bundesamt für Sicherheit in der Informationstechnik
Kristin Brandt	Bundesamt für Sicherheit in der Informationstechnik
René Costa	Bundesamt für Sicherheit in der Informationstechnik
Sören Dietrich	Bundesamt für Sicherheit in der Informationstechnik
Angelika Haas	Bundesministerium für Ernährung und Landwirtschaft
Birger Klein	Bundesamt für Sicherheit in der Informationstechnik
Patrick Muhl	Bundesamt für Sicherheit in der Informationstechnik
Christoph Möhring	Bundesministerium für Wohnen, Stadtentwicklung und Bauwesen
Hans-Christian Ortholf	Bundesministerium der Justiz

*Tabelle 2: Liste der Autorinnen und Autoren*

Das IT-Grundschutz-Profil wurde mit Unterstützung der Maßnahmenleitung der E-Akte Bund erstellt.

Sollten Sie bei der Anwendung des IT-Grundschutz-Profiles Anmerkungen oder Ergänzungen haben oder möchten Sie an einer Weiterentwicklung des IT-Grundschutz-Profiles mitarbeiten, wenden Sie sich bitte an [sicherheitsberatung@bsi.bund.de](mailto:sicherheitsberatung@bsi.bund.de).

## **5 Management Summary**

### **5.1 Zielgruppe**

Dieses IT-Grundschutz-Profil richtet sich an die für das Informationssicherheitsmanagement Zuständigen in den die E-Akte Bund nutzenden Behörden und Einrichtungen der Bundesregierung und der unmittelbaren Bundesverwaltung.

### **5.2 Zielsetzung**

Das IT-Grundschutz-Profil soll den Nutzerbehörden dabei helfen, die E-Akte Bund entsprechend ihren jeweiligen Sicherheitsanforderungen zu nutzen.

Es nimmt hierzu Abgrenzungen hinsichtlich der Zuständigkeiten bzw. Verantwortungsbereiche vor und beschreibt die ggf. erforderlichen Schnittstellen.

Das IT-Grundschutz-Profil soll als Blaupause für die Erstellung und Umsetzung eines fachspezifischen Sicherheitskonzepts zur E-Akte-Nutzung und dessen Integration in die übergreifende Sicherheitskonzeption der Behörde dienen.

### **5.3 Abdeckung Vorgehensweise**

Die in diesem IT-Grundschutz-Profil beschriebenen Anforderungen entsprechen der Vorgehensweise „Standard-Absicherung“ des BSI-Standards 200-2.

### **5.4 ISO 27001-Kompatibilität**

Durch die Umsetzung der Standard-Absicherung besteht Kompatibilität zur ISO/IEC 27001.

### **5.5 Aufgaben der Leitungsebene**

Im Rahmen ihrer Gesamtverantwortung für die Informationssicherheit ist es die Aufgabe der obersten Leitungsebene der jeweiligen Nutzerbehörde die Umsetzung der sich aus diesem IT-Grundschutz-Profil und dem daraus abgeleiteten Sicherheitskonzept ergebenden Anforderungen in ihrem Zuständigkeitsbereich zu initiieren, zu steuern und zu kontrollieren.

Sie muss die dazu benötigten personellen und materiellen Ressourcen bereitstellen sowie die dafür erforderlichen organisatorischen Voraussetzungen schaffen.



## **6 Festlegung des Geltungsbereichs**

### **6.1 Beschreibung des Schutzbedarfs**

Der Schutzbedarf kann in den die E-Akte Bund nutzenden Behörden und Einrichtungen unterschiedlich ausgeprägt sein. Im vorliegenden IT-Grundschutz-Profil wird grundlegend von einem Schutzbedarf in der Ausprägung „Normal“ in den drei Schutzzielen Vertraulichkeit, Integrität und Verfügbarkeit ausgegangen.

Im Rahmen einer von Anwendenden des IT-Grundschutz-Profiles durchzuführenden individuellen Schutzbedarfsfeststellung für die jeweilige Behörde bzw. Einrichtung kann möglicherweise ein höherer Schutzbedarf festgestellt werden. Dieser ist bei der Ableitung eines Sicherheitskonzeptes nach diesem IT-Grundschutz-Profil individuell zu berücksichtigen.

### **6.2 Abgrenzung des Informationsverbundes**

#### **6.2.1 Beschreibung des Musterszenarios**

Die im BSI-Standard 200-2 beschriebene IT-Grundschutz-Methodik sieht vor, dass die Bestandteile (Zielobjekte) des zu untersuchenden Informationsverbunds ausgehend von den Geschäftsprozessen bzw. Fachaufgaben erhoben werden, für deren Unterstützung diese Zielobjekte benötigt werden.

Für sich genommen stellt die Nutzung der E-Akte Bund für das elektronische Dokumentenmanagement und die Vorgangsbearbeitung der Nutzerbehörde keinen eigenständigen Geschäftsprozess dar, sondern ist eine Anwendung zur Unterstützung verschiedenster Geschäftsprozesse bzw. Fachaufgaben. Das Musterszenario des vorliegenden IT-Grundschutz-Profiles geht deshalb aus von einem abstrakten, nicht weiter spezifizierten Kern- oder Führungsprozess<sup>1</sup> der Nutzerbehörde, zu dessen Unterstützung die E-Akte Bund genutzt wird.

Bei der Anwendung des IT-Grundschutz-Profiles zur Erstellung eines behördenspezifischen Sicherheitskonzeptes, insbesondere bei der Schutzbedarfsfeststellung, ist dieser abstrakte Geschäftsprozess durch einen oder mehrere reale Geschäftsprozesse bzw. Fachaufgaben der Nutzerbehörde (bspw. Vorbereitung von Gesetzentwürfen oder Beschaffung von Dienstleistungen) zu ersetzen.

---

<sup>1</sup> Zur Erläuterung der Begriffe Führungs-, Kern- und Unterstützungsprozess siehe [9], S. 10, bzw. 10.4 Glossar.

## 6.2.2 Beschreibung des Informationsverbunds

Der diesem IT-Grundschutz-Profil zugrundeliegende **Informationsverbund** umfasst grundsätzlich alle organisatorischen Strukturen, Geschäftsprozesse und Anwendungen sowie IT-Systeme, Netze, Kommunikationsverbindungen und (baulichen) Infrastrukturen, die für die Nutzung der E-Akte Bund im Zuständigkeitsbereich der Nutzerbehörde benötigt werden. Dazu gehören auch Dienste und IT-Systeme der Nutzerbehörde, die zur Anbindung und Authentisierung an die zugehörigen E-Akte-Mandanten in der Produktions- und Integrationsumgebung beim ITZBund benötigt werden.

Anwendende dieses IT-Grundschutz-Profiles müssen prüfen, ob alle für sie relevanten Aspekte in der Referenzarchitektur abgebildet sind. Existieren aufgrund der konkreten Geschäftsprozesse weitere oder andere Bestandteile des Informationsverbundes, so sind diese in den Informationsverbund aufzunehmen.

**Nicht zum Informationsverbund** gehören die zentralen, beim ITZBund betriebenen Dienste der E-Akte Bund, die zu deren Bereitstellung benötigten IT-Systeme, Netze und Kommunikationsverbindungen einschließlich der E-Akte-Mandanten der Nutzerbehörde, sowie die vom ITZBund bereitgestellten Schnittstellen zu anderen zentralen Diensten des Bundes.

**Nicht berücksichtigt** werden weiterhin andere, im Rahmen der E-Akte-Nutzung in Anspruch genommene Dienste sowie ausgelagerte Geschäftsprozesse (bspw. Digitalisierungsdienstleistung nach BSI-TR 03138 [5]).

## 6.3 Strukturanalyse

### 6.3.1 Geschäftsprozesse / Fachaufgaben

ID	Geschäftsprozesse / Fachaufgaben	Prozessart	Beschreibung
GP01	Geschäftsprozess / Fachaufgabe mit Nutzung der E-Akte Bund	Kern- oder Führungsprozess	Abstrakter, nicht weiter spezifizierter Kern- oder Führungsprozess der Nutzerbehörde
GP02	Digitalisierung Posteingang	Unterstützungs- prozess	Digitalisierung eingehender Papierdokumente (Scannen)
GP03	Fachliche Administration	Unterstützungs- prozess	Benutzer- und Rechteverwaltung für die E-Akte-Nutzung; Integration von in anderen Fachverfahrenen erstellten Formularen über definierte Schnittstellen etc.
GP04	Technische Administration	Unterstützungs- prozess	Prüfung der Schnittstellen und Integrationsmuster; Arbeit an den Wartungszugängen zu den Produktivmandanten etc.
GP05	IT-Betrieb	Unterstützungs- prozess	Tätigkeiten, die durch die Organisationseinheit IT-Betrieb in der Nutzerbehörde durchgeführt werden; falls die Nutzerbehörde im Rahmen der ITKB vollkonsolidiert ist, entfällt dieser Geschäfts- prozess

Tabelle 3: Geschäftsprozesse / Fachaufgaben

## 6.3.2 Netzplan

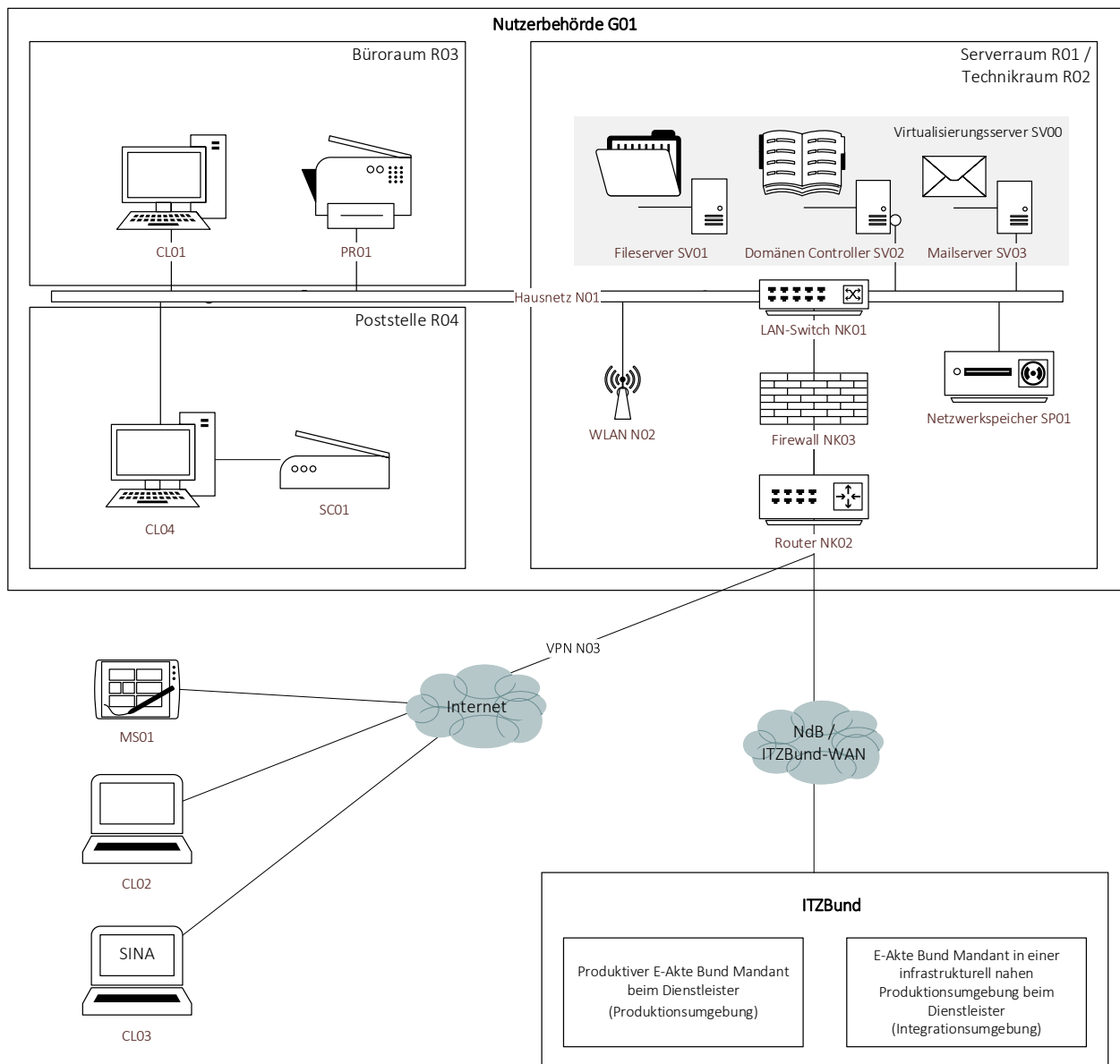


Abbildung 1: Vereinfachter Netzplan für das Musterszenario

### 6.3.3 Anwendungen

ID	Anwendungen	Beschreibung	Zuordnung zu Prozessen
A01	Active Directory	Nutzer-, Rollen- und Rechteverwaltung der Nutzerbehörde	GP01, GP05
A02	Mail Service	E-Mail-Dienst der Nutzerbehörde	GP01
A03	Fileservice	Lokale Dateiablage der Nutzerbehörde	GP01
A04	Name Service	DNS-Service auf dem DC SV02	GP01
A05	Fabasoft Folio Client	Client-Anwendung für den Zugriff auf die E-Akte Bund (optional)	GP01
A06	Office	Beliebiges Office-Paket (Microsoft, Open, Libre etc.), das lokal auf CL01, CL02 oder CL03 installiert ist	GP01
A07	Browser	Beliebige Webbrowser auf CL01, CL02 oder CL03 (bspw. Edge, Chrome, Firefox) sowie MS01 (bspw. Safari, Chrome)	GP01, GP03, GP04, GP05
A08	Diverse Client-Anwendungen	Governikus Communicator, DE-Mail Plugin, eNorm-Add-on, Folio-Mail-Add-in etc.	GP01
A09	Scan-Software	TR-03138-konforme Lösung zur beweiswerterhaltenden Digitalisierung von Papierdokumenten	GP02

Tabelle 4: Anwendungen

### 6.3.4 IT-Systeme

ID	IT-Systeme	Beschreibung	Zuordnung zu Anwendungen
CL01	Client	Arbeitsplatz-Clients der Nutzenden	A05, A06, A07, A08
CL02	Laptop	mobile Arbeitsplatz-Clients der Nutzenden	A05, A06, A07, A08
CL03	SINA-Laptop	mobile Arbeitsplatz-Clients der Nutzenden mit SINA Workstation	A05, A06, A07, A08
CL04	Scan-AP	Scan-Arbeitsplatz für die Digitalisierung	A09
MS01	Tablet	mobile IT-Systeme, sofern diese Zugriff auf die E-Akte haben	A02, A07
SV00	Virtualisierungsserver	wenn ein oder mehrere der Server SV01 - SV03 virtualisiert sind (optional)	-
SV01	Fileserver	Server, auf dem der Fileservice (Dateiablage) bereitgestellt wird	A03
SV02	Domänen Controller	Server, auf dem das Active Directory und der DNS bereitgestellt werden	A01, A04
SV03	Mailserver	Server, auf dem der Mail-Service bereitgestellt wird	A02
SP01	Speichersystem	SAN/NAS für den Fileservice	A03
PR01	Multifunktionsgerät	Drucker, Kopierer	A05, A06, A07, A08
SC01	Scanner	an CL04 angeschlossener Scanner zur Digitalisierung	A09

Tabelle 5: IT-Systeme

### 6.3.5 Netze und Netzkomponenten

ID	Netze und Netzkomponenten	Zuordnung zu IT-Systemen
N01	Hausnetz der Nutzerbehörde	CL01, CL02, CL03, CL04, SV00, SV01, SV02, SV03, SP01, PR01, SC01
N02	WLAN der Nutzerbehörde	CL02, CL03, MS01
N03	VPN zur Anbindung der Laptops und mobilen IT-Systeme an das Hausnetz der Nutzerbehörde über das Internet	CL02, CL03, MS01
N04	Anbindung der Nutzerbehörde an NdB	-
N05	Anbindung der Nutzerbehörde an ITZBund-WAN	-
N06	Internetanbindung der Nutzerbehörde	-
NK01	Switch im Hausnetz (gruppiert)	-
NK02	Router zur Internetanbindung	-
NK03	Firewall	-

Tabelle 6: Netze und Netzkomponenten

### 6.3.6 Gebäude und Räume

ID	Gebäude oder Raum	Zuordnung zu IT-Systemen / Netzkomponenten
G01	Gebäude der Nutzerbehörde	-
R01	Serverraum	SV00, SV01, SV02, SV03, SP01, NK01, NK02, NK03
R02	Technikraum	NK01
R03	Büroraum	CL01, CL02, MS01, PR01
R04	Poststelle	CL04, SC01
R05	Besprechungsraum	CL02, CL03, MS01
R06	Heimarbeitsplatz	CL02, CL03, MS01
R07	Mobiler Arbeitsplatz	CL02, CL03, MS01

Tabelle 7: Gebäude und Räume

## **6.4 Umgang mit Abweichungen**

Weicht der zu schützende Informationsverbund von dem Musterszenario ab, sind die zusätzlichen oder nicht vorhandenen Zielobjekte zu dokumentieren. Den zusätzlichen Zielobjekten sind geeignete Bausteine des IT-Grundschutz-Kompendiums zuzuordnen.

In Abschnitt 9.3 werden Hinweise zur Anwendung der modellierten Bausteine gegeben, die auch mögliche Abweichungen vom Musterszenario berücksichtigen.



## **7 Zu erfüllende Anforderungen und umzusetzende Maßnahmen**

### **7.1 Feststellung des Schutzbedarfs**

Durch die Nutzerbehörde ist für die in eigener Zuständigkeit befindlichen Geschäftsprozesse, Anwendungen, IT-Systeme, Netze und Kommunikationsverbindungen sowie Infrastrukturobjekte eine individuelle Schutzbedarfsfeststellung gemäß BSI-Standard 200-2 durchzuführen. Der Schutzbedarfsfeststellung sind die Schutzbedarfskategorien zu Grunde zu legen, die im Mindeststandard des BSI für das ISMS ITKB [6] festgelegt sind.<sup>2</sup> Der abstrakte Geschäftsprozess GP01 ist dabei durch einen oder mehrere konkrete Geschäftsprozesse zu ersetzen.

Bei der Vererbung des Schutzbedarfs von GP01 auf die Zielobjekte des Informationsverbunds sind darüber hinaus etwaige Kumulationseffekte zu berücksichtigen, um in der Bewertung nicht nur einzelne Akten, sondern auch Zusammenstellungen von Akten zu erfassen.

Überschreitet der durch die Nutzerbehörde individuell festgestellte Schutzbedarf das vom ITZBund gewährleistete Schutzniveau, so darf die Nutzerbehörde nur auf Grundlage einer Risikoanalyse entscheiden, ob die E-Akte Bund wie bereitgestellt genutzt werden kann.

### **7.2 Zuordnung der relevanten Bausteine**

Nachdem die Referenzarchitektur mit den entsprechenden Zielobjekten definiert ist und die Schutzbedarfsfeststellung durchgeführt wurde, besteht die nächste Aufgabe darin, den betrachteten Informationsverbund mit Hilfe des IT-Grundschutz-Modells nachzubilden. Dafür werden die Bausteine des IT-Grundschutz-Kompendiums auf ihre Relevanz geprüft und ggf. auf die jeweiligen Zielobjekte abgebildet (siehe auch BSI-Standard 200-2, Kapitel 8.3 oder Kapitel 2 des IT-Grundschutz-Kompendiums).

---

<sup>2</sup> Der Mindeststandard des BSI für das ISMS ITKB befindet sich aktuell in Erstellung. Bis zu seinem Inkrafttreten gilt das vorläufige Regelungsdokument 4.0 [7].

## Modellierung

Baustein	Relevant Ja/Nein	Anzuwenden auf oder Begründung, falls nicht relevant
ISMS.1 Sicherheitsmanagement	Ja	Informationsverbund
ORP.1 Organisation	Ja	Informationsverbund
ORP.2 Personal	Ja	Informationsverbund
ORP.3 Sensibilisierung und Schulung zur Informationssicherheit	Ja	Informationsverbund
ORP.4 Identitäts- und Berechtigungsmanagement	Ja	Informationsverbund
ORP.5 Compliance Management (Anforderungsmanagement)	Ja	Informationsverbund
CON.1 Kryptokonzept	Ja	Informationsverbund
CON.2 Datenschutz	Ja	Informationsverbund, falls personenbezogene Daten verarbeitet werden
CON.3 Datensicherungskonzept	Ja	Informationsverbund
CON.6 Löschen und Vernichten	Ja	Informationsverbund
CON.7 Informationssicherheit auf Auslandsreisen	Ja	Informationsverbund
CON.8 Software-Entwicklung	Nein	Nicht im Geltungsbereich.
CON.9 Informationsaustausch	Ja	Informationsverbund
CON.10 Entwicklung von Webanwendungen	Nein	Nicht im Geltungsbereich.
CON.11.1 Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)	Ja	Informationsverbund, falls VS-NfD verarbeitet wird
OPS.1.1.1 Allgemeiner IT-Betrieb	Ja	Informationsverbund
OPS.1.1.2 Ordnungsgemäße IT- Administration	Ja	Informationsverbund
OPS.1.1.3 Patch- und Änderungsmanagement	Ja	Informationsverbund
OPS.1.1.4 Schutz vor Schadprogrammen	Ja	Informationsverbund

Baustein	Relevant Ja/Nein	Anzuwenden auf oder Begründung, falls nicht relevant
OPS.1.1.5 Protokollierung	Ja	Informationsverbund
OPS.1.1.6 Software-Tests und -Freigaben	Ja	Informationsverbund
OPS.1.1.7 Systemmanagement	Ja	die konkrete Systemmanagement- lösung, wenn eine solche eingesetzt wird
OPS.1.2.2 Archivierung	Nein	Nicht im Geltungsbereich.
OPS.1.2.4 Telearbeit	Ja	jeden Telearbeitsplatz, wenn Telearbeit genutzt wird
OPS.1.2.5 Fernwartung	Ja	alle Zielobjekte, die von der Nutzerbehörde oder von Dritten ferngewartet werden
OPS.1.2.6 NTP-Zeitsynchronisation	Ja	alle IT-Systeme im Informationsverbund, die NTP nutzen
OPS.2.2 Cloud-Nutzung	Nein	Nach [6], ISMS-ITKB.2.9.01, soll der Baustein OPS.2.2 nicht für Leistungen der ITKB angewendet werden.
OPS.2.3 Nutzung von Outsourcing	Nein	Nach [6], ISMS-ITKB.2.9.01, soll der Baustein OPS.2.3 nicht für Leistungen der ITKB angewendet werden.
OPS.3.2 Anbieten von Outsourcing	Nein	Nach [6], ISMS-ITKB.2.9.01, soll der Baustein OPS.3.2 nicht für Leistungen der ITKB angewendet werden.
OPS.bd.3.1 Leistungsbeziehung in der IT-Konsolidierung Bund (ITKB)	Ja	jede in Anspruch genommene Leistung der ITKB (siehe [6], ISMS-ITKB.2.9.01)
DER.1 Detektion von sicherheitsrelevanten Ereignissen	Ja	Informationsverbund
DER.2.1 Behandlung von Sicherheitsvorfällen	Ja	Informationsverbund
DER.2.2 Vorsorge für die IT-Forensik	Ja	Informationsverbund
DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle	Nein	Reaktiver Baustein, der erst nach einem APT-Vorfall anzuwenden ist.
DER.3.1 Audits und Revisionen	Nein	Abgedeckt durch Baustein DER.3.2.

Baustein	Relevant Ja/Nein	Anzuwenden auf oder Begründung, falls nicht relevant
DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision	Ja	Informationsverbund
DER.4 Notfallmanagement	Ja	Informationsverbund
APP.1.1 Office-Produkte	Ja	A06
APP.1.2 Web-Browser	Ja	A07
APP.1.4 Mobile Anwendungen (Apps)	Nein	Nicht im Geltungsbereich.
APP.2.1 Allgemeiner Verzeichnisdienst	Ja	A01
APP.2.2 Active Directory	Ja	A01
APP.2.3 OpenLDAP	Nein	Nicht im Einsatz.
APP.3.1 Webanwendungen und Webservices	Nein	Nicht im Einsatz.
APP.3.2 Webserver	Nein	Nicht im Einsatz.
APP.3.3 Fileserver	Ja	A03
APP.3.4 Samba	Nein	Nicht im Einsatz.
APP.3.6 DNS-Server	Ja	A04
APP.4.2 SAP-ERP-System	Nein	Nicht im Einsatz.
APP.4.3 Relationale Datenbanksysteme	Nein	Nicht im Geltungsbereich.
APP.4.4 Kubernetes	Nein	Nicht im Einsatz.
APP.4.6 SAP ABAP-Programmierung	Nein	Nicht im Einsatz.
APP.5.2 Microsoft Exchange und Outlook	Ja	A02
APP.5.3 Allgemeiner E-Mail-Client und -Server	Ja	A02
APP.6 Allgemeine Software	Ja	A01 - A09
APP.7 Entwicklung von Individualsoftware	Nein	Nicht im Geltungsbereich.
SYS.1.1 Allgemeiner Server	Ja	SV00, SV01, SV02, SV03
SYS.1.2.2 Windows Server 2012	Nein	Nicht im Einsatz.

Baustein	Relevant Ja/Nein	Anzuwenden auf oder Begründung, falls nicht relevant
SYS.1.2.3 Windows Server	Ja	SV01, SV02, SV03
SYS.1.3 Server unter Linux und Unix	Nein	Nicht im Einsatz.
SYS.1.5 Virtualisierung	Ja	SV00, falls einer der Server SV01, SV02 oder SV03 virtualisiert ist
SYS.1.6 Containerisierung	Nein	Nicht im Einsatz.
SYS.1.7 IBM Z	Nein	Nicht im Einsatz.
SYS.1.8 Speicherlösungen	Ja	SP01
SYS.1.9 Terminalserver	Nein	Nicht im Einsatz.
SYS.2.1 Allgemeiner Client	Ja	CL01 - CL04
SYS.2.2.3 Clients unter Windows	Ja	CL01, CL02, CL04
SYS.2.3 Clients unter Linux und Unix	Ja	CL03
SYS.2.4 Clients unter macOS	Nein	Nicht im Einsatz.
SYS.2.5 Client-Virtualisierung	Nein	Nicht im Einsatz.
SYS.2.6 Virtual Desktop Infrastructure	Nein	Nicht im Einsatz.
SYS.3.1 Laptops	Ja	CL02, CL03
SYS.3.2.1 Allgemeine Smartphones und Tablets	Ja	MS01
SYS.3.2.2 Mobile Device Management (MDM)	Ja	Informationsverbund, wenn ein MDM im Einsatz ist
SYS.3.2.3 iOS (for Enterprise)	Ja	MS01, wenn die Tablets unter iOS laufen
SYS.3.2.4 Android	Ja	MS01, wenn die Tablets unter Android laufen
SYS.3.3 Mobiltelefon	Nein	Nicht im Geltungsbereich.
SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte	Ja	PR01, SC01
SYS.4.3 Eingebettete Systeme	Nein	Nicht im Einsatz.
SYS.4.4 Allgemeines IoT-Gerät	Nein	Nicht im Einsatz.

Baustein	Relevant Ja/Nein	Anzuwenden auf oder Begründung, falls nicht relevant
SYS.4.5 Wechseldatenträger	Ja	alle Wechseldatenträger im Informationsverbund
NET.1.1 Netzarchitektur und -design	Ja	N01
NET.1.2 Netzmanagement	Ja	die konkrete Netzmanagementlösung, wenn eine solche eingesetzt wird
NET.2.1 WLAN-Betrieb	Ja	N02
NET.2.2 WLAN-Nutzung	Ja	CL02, CL03, MS01
NET.3.1 Router und Switches	Ja	NK01, NK02
NET.3.2 Firewall	Ja	NK03
NET.3.3 VPN	Ja	N03
NET.3.4 Network Access Control	Nein	Nicht im Einsatz.
NET.4.1 TK-Anlagen	Nein	Nicht im Geltungsbereich.
NET.4.2 VoIP	Nein	Nicht im Geltungsbereich.
NET.4.3 Faxgeräte und Faxserver	Nein	Nicht im Geltungsbereich.
IND.1 Prozessleit- und Automatisierungstechnik	Nein	Nicht im Einsatz.
IND.2.1 Allgemeine ICS-Komponente	Nein	Nicht im Einsatz.
IND.2.2 Speicherprogrammierbare Steuerung (SPS)	Nein	Nicht im Einsatz.
IND.2.3 Sensoren und Aktoren	Nein	Nicht im Einsatz.
IND.2.4 Maschine	Nein	Nicht im Einsatz.
IND.2.7 Safety Instrumented Systems	Nein	Nicht im Einsatz.
IND.3.2 Fernwartung im industriellen Umfeld	Nein	Nicht im Einsatz.
INF.1 Allgemeines Gebäude	Ja	G01
INF.2 Rechenzentrum sowie Serverraum	Ja	R01

Baustein	Relevant Ja/Nein	Anzuwenden auf oder Begründung, falls nicht relevant
INF.5 Raum sowie Schrank für technische Infrastruktur	Ja	R02 sowie R01, falls es sich um einen Serverraum mit wenigen IT-Systemen handelt (siehe Baustein INF.2, Abschn. 1.3)
INF.6 Datenträgerarchiv	Nein	Nicht im Geltungsbereich.
INF.7 Büroarbeitsplatz	Ja	R03, R04
INF.8 Häuslicher Arbeitsplatz	Ja	R06
INF.9 Mobiler Arbeitsplatz	Ja	R07
INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume	Ja	R05
INF.11 Allgemeines Fahrzeug	Nein	Nicht im Geltungsbereich.
INF.12 Verkabelung	Ja	G01
INF.13 Technisches Gebäudemanagement	Nein	Nicht im Geltungsbereich.
INF.14 Gebäudeautomatisierung	Nein	Nicht im Geltungsbereich.

*Tabelle 8: Modellierung der Bausteine*

### 7.3 Relevanz der Anforderungen

Bei der Anwendung des IT-Grundschutz-Profiles für die Nutzung der E-Akte Bund sind grundsätzlich alle relevanten Basis- und Standard-Anforderungen der modellierten Bausteine des IT-Grundschutz-Kompendiums zu erfüllen.

## 8 Risikoanalyse / Restrisiko

Wenn bei der Anwendung des IT-Grundschutz-Profiles im Rahmen der individuellen Schutzbedarfsfeststellung durch die Nutzerbehörde Zielobjekte mit erhöhtem Schutzbedarf identifiziert wurden, ist für diese eine Risikoanalyse durchzuführen.

Risiken ergeben sich auch daraus, dass relevante Anforderungen aus den modellierten Bausteinen nicht oder nur teilweise erfüllt werden.

Zur Durchführung der Risikoanalyse nach dem BSI-Standard 200-3 sind aus den dort beschriebenen 47 elementaren Gefährdungen diejenigen auszuwählen, die für die jeweiligen Zielobjekte direkt relevant sind. Direkt relevant ist eine Gefährdung dann, wenn sie unmittelbar auf das jeweilige Zielobjekt wirken kann.

Im Hilfsdokument zur Risikoanalyse [8] sind alle elementaren Gefährdungen aufgelistet und diejenigen, die sich aus der Nutzung der E-Akte Bund für den Informationsverbund ergeben, als „direkt relevant“ gekennzeichnet. Diese Liste muss gegebenenfalls behördenspezifisch ergänzt und erweitert werden.



## 9 Anwendungshinweise

### 9.1 Anwendung in vollständig konsolidierten Nutzerbehörden

Bei der Anwendung des IT-Grundschutz-Profiles in Nutzerbehörden, die im Rahmen der IT-Betriebskonsolidierung Bund (BKB) vollständig konsolidiert sind, liegt die Umsetzung der in Abschnitt 7.2 als relevant ermittelten Bausteine der Schichten OPS, APP, SYS und NET in der Zuständigkeit des ITZBund.

### 9.2 Anwendung in nicht oder teilweise konsolidierten Nutzerbehörden

Bei der Anwendung des IT-Grundschutz-Profiles in Nutzerbehörden, die im Rahmen der IT-Betriebskonsolidierung Bund (BKB) nicht oder nicht vollständig konsolidiert sind, kann für die in Abschnitt 7.2 als relevant ermittelten Bausteine auf das übergreifende Sicherheitskonzept der Nutzerbehörde referenziert werden, sofern

- dieses in einer aktuellen Fassung vorliegt,
- die betreffenden Bausteine darin vollständig bearbeitet und dokumentiert sind,
- sich aus den betreffenden Baustein-Anforderungen keine für die Nutzung der E-Akte spezifischen Maßnahmen ergeben.

### 9.3 Hinweise zu einzelnen Bausteinen

Bei der Anwendung der Bausteine können die Hilfsmittel aus dem Werkzeugkasten der Sicherheitsberatung genutzt werden (siehe (3)).

Zu einigen Bausteinen werden im Folgenden hilfreiche Anwendungshinweise gegeben.

Baustein	Zuständig für die Umsetzung	Anwendungshinweise
ISMS.1 Sicherheitsmanagement	ISB, Behördenleitung	-
ORP.1 Organisation	Zentrale Verwaltung gemäß GVP	-
ORP.2 Personal	Personalabteilung	-
ORP.3 Sensibilisierung und Schulung zur Informationssicherheit	ISB	Bei der Anwendung des Bausteins ist besonders auf die Eigenverantwortlichkeit der Beschäftigten für die Einstufung der Akten einzugehen.

Baustein	Zuständig für die Umsetzung	Anwendungshinweise
ORP.4 Identitäts- und Berechtigungsmanagement	ISB, IT-Betrieb	-
ORP.5 Compliance Management (Anforderungsmanagement)	Compliance, Justizariat	-
CON.1 Kryptokonzept	ISB	Der Baustein muss u. a. angewendet werden, wenn ein VPN eingesetzt wird oder Dokumente elektronisch signiert werden.
CON.2 Datenschutz	Behördenleitung, DSB	-
CON.3 Datensicherungskonzept	ISB, IT-Betrieb	-
CON.6 Löschen und Vernichten	ISB, IT-Betrieb	Bei der Anwendung des Bausteins müssen besonders die gesetzlichen Lösch- und Aufbewahrungsfristen beachtet werden.
CON.7 Informationssicherheit auf Auslandsreisen	ISB	-
CON.9 Informationsaustausch	ISB	-
CON.11.1 Geheimchutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)	GSB	Für die Anwendung dieses Bausteins sind die Geheimchutzbeauftragten der Nutzerbehörden zuständig.
OPS.1.1.1 Allgemeiner IT-Betrieb	IT-Betrieb	-
OPS.1.1.2 Ordnungsgemäße IT-Administration	IT-Betrieb	-

Baustein	Zuständig für die Umsetzung	Anwendungshinweise
OPS.1.1.3 Patch- und Änderungsmanagement	IT-Betrieb	Bei der Anwendung des Bausteins müssen die entsprechenden Vorgaben und Abläufe des ITZBund berücksichtigt werden.
OPS.1.1.4 Schutz vor Schadprogrammen	IT-Betrieb	-
OPS.1.1.5 Protokollierung	IT-Betrieb	-
OPS.1.1.6 Software-Tests und -Freigaben	IT-Betrieb	-
OPS.1.1.7 Systemmanagement	IT-Betrieb	-
OPS.1.2.4 Telearbeit	ISB	Der Baustein wird nur auf Telearbeit angewendet, wenn diese im Arbeitsvertrag oder in einer Dienstvereinbarung geregelt ist. Zusätzlich ist dann der Baustein INF.8 Häuslicher Arbeitsplatz anzuwenden.
OPS.1.2.5 Fernwartung	IT-Betrieb	Bei der Anwendung des Bausteins ist zu beachten, dass er nicht in erster Linie die Fernwartung über Weitverkehrsnetze sondern innerhalb des Hausnetzes behandelt.
OPS.1.2.6 NTP - Zeitsynchronisation	IT-Betrieb	-
DER.1 Detektion von sicherheitsrelevanten Ereignissen	IT-Betrieb	-
DER.2.1 Behandlung von Sicherheitsvorfällen	ISB, IT-Betrieb	-

Baustein	Zuständig für die Umsetzung	Anwendungshinweise
DER.2.2 Vorsorge für die IT-Forensik	ISB	-
DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision	ISB, Behördenleitung	Gemäß UP Bund 2017 sind Bundesbehörden dazu verpflichtet, ihr ISMS durch IS-Revisionen zu überprüfen. Sollte eine Nutzerbehörde nicht dem UP Bund 2017 unterliegen, ist anstelle des Bausteins DER.3.2 der Baustein DER.3.1 Audits und Revisionen anzuwenden.
DER.4 Notfallmanagement	NFB	Bei der Anwendung des Bausteins ist besonders auf die Einbeziehung des ITZBund in die Konzeption der Notfallvorsorge und Notfallreaktion zu achten.
APP.1.1 Office-Produkte	IT-Betrieb	Der Baustein ist nur auf lokal installierte Office-Anwendungen anzuwenden. Cloudbasierte Office-Produkte (bspw. Microsoft 365) sind nicht erfasst; auf diese ist der Baustein OPS.2.2 Cloud-Nutzung anzuwenden.
APP.1.2 Web-Browser	IT-Betrieb	Bei der Anwendung des Bausteins sollte auch der Mindeststandard des BSI für Webbrowser beachtet werden.
APP.2.1 Allgemeiner Verzeichnisdienst	IT-Betrieb	-

Baustein	Zuständig für die Umsetzung	Anwendungshinweise
APP.2.2 Active Directory	IT-Betrieb	Sollte anstelle von Active Directory Open LDAP als Verzeichnisdienst genutzt werden, ist der Baustein APP.2.3 OpenLDAP anzuwenden. Im Falle eines anderen Verzeichnisdienstes sollte eine individuelle Risikoanalyse in Erwägung gezogen werden.
APP.3.3 Fileserver	IT-Betrieb	-
APP.3.6 DNS-Server	IT-Betrieb	-
APP.5.2 Microsoft Exchange und Outlook	IT-Betrieb	Im Falle des Einsatzes eines anderen E-Mail-Dienstes sollte eine individuelle Risikoanalyse in Erwägung gezogen werden.
APP.5.3 Allgemeiner E-Mail-Client und -Server	IT-Betrieb	-
APP.6 Allgemeine Software	IT-Betrieb	-
SYS.1.1 Allgemeiner Server	IT-Betrieb	-
SYS.1.2.3 Windows Server	IT-Betrieb	Wenn anstelle oder neben Servern unter Windows Server unter Linux oder Unix betrieben werden, ist der Baustein SYS.1.3 Server unter Linux und Unix anzuwenden.
SYS.1.5 Virtualisierung	IT-Betrieb	Wenn der zur Virtualisierung eingesetzte Hypervisor ein Betriebssystem voraussetzt (bspw. Hyper-V oder Proxmox), muss auf SV00 auch der entsprechende Betriebssystem-Baustein angewendet werden.
SYS.1.8 Speicherlösungen	IT-Betrieb	-

Baustein	Zuständig für die Umsetzung	Anwendungshinweise
SYS.2.1 Allgemeiner Client	IT-Betrieb	-
SYS.2.2.3 Clients unter Windows	IT-Betrieb	Wenn anstelle oder neben Clients unter Windows Clients unter Linux oder Unix betrieben werden, ist der Baustein SYS.2.3 Clients unter Linux und Unix anzuwenden.
SYS.2.3 Clients unter Linux und Unix	IT-Betrieb	Auf den SINA-Laptop CL03 sollte zusätzlich der benutzerdefinierte Baustein SYS.bd.3: SINA Endgerät angewendet werden.
SYS.3.1 Laptops	IT-Betrieb	-
SYS.3.2.1 Allgemeine Smartphones und Tablets	IT-Betrieb	Wenn Tablets MS01 im Informationsverbund über eine Mobilfunktion (SIM-Karte) verfügen, sollte für diese Geräte zusätzlich der Baustein SYS.3.3 Mobiltelefon angewendet werden.
SYS.3.2.2 Mobile Device Management (MDM)	IT-Betrieb	-
SYS.3.2.3 iOS (for Enterprise)	IT-Betrieb	-
SYS.3.2.4 Android	IT-Betrieb	-
SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte	IT-Betrieb	Bei der Anwendung des Bausteins auf den Scanner SC01 zur Digitalisierung sind zusätzlich die Anforderungen der BSI TR-03138 Ersetzendes Scannen zu erfüllen.
SYS.4.5 Wechseldatenträger	IT-Betrieb	-

Baustein	Zuständig für die Umsetzung	Anwendungshinweise
NET.1.1 Netzarchitektur und -design	IT-Betrieb	Der Baustein muss nur einmal auf das gesamte Hausnetz der Nutzerbehörde angewendet werden.
NET.1.2 Netzmanagement	IT-Betrieb	-
NET.2.1 WLAN-Betrieb	IT-Betrieb	-
NET.2.2 WLAN-Nutzung	IT-Betrieb	Der Baustein ist auf die mobilen IT-Systeme CL02, CL03, MS01 anzuwenden, auch wenn kein eigenes WLAN betrieben wird.
NET.3.1 Router und Switches	IT-Betrieb	Der Baustein muss nur auf die in der Zuständigkeit der Nutzerbehörde befindlichen Switches bzw. Router angewendet werden.
NET.3.2 Firewall	IT-Betrieb	Werden mehrere Firewalls zu unterschiedlichen Zwecken eingesetzt, ist der Baustein auf jedes einzelne Firewall-Objekt anzuwenden.
NET.3.3 VPN	IT-Betrieb	-
INF.1 Allgemeines Gebäude	FM, Haustechnik	-
INF.2 Rechenzentrum sowie Serverraum	IT-Betrieb, Haustechnik	Der Baustein eignet sich nicht für kleine Informationsverbünde mit nur sehr wenigen Servern oder IT-Systemen. In solchen Fällen genügt es, den Baustein INF.5 Raum sowie Schrank für technische Infrastruktur anzuwenden. Die Entscheidung darüber obliegt dem ISB der Nutzerbehörde.

Baustein	Zuständig für die Umsetzung	Anwendungshinweise
INF.5 Raum sowie Schrank für technische Infrastruktur	IT-Betrieb, Haustechnik	-
INF.7 Büroarbeitsplatz	ISB	-
INF.8 Häuslicher Arbeitsplatz	Beschäftigte	Der Baustein ist nur zusätzlich zum Baustein OPS.1.2.4 Telearbeit anzuwenden.
INF.9 Mobiler Arbeitsplatz	ISB	-
INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume	Zentrale Verwaltung	-
INF.12 Verkabelung	IT-Betrieb, Haustechnik	-

*Tabelle 9: Anwendungshinweise*



## 10 Anhang

### 10.1 Verzeichnisse

#### 10.1.1 Abbildungsverzeichnis

Abbildung 1: Vereinfachter Netzplan für das Musterszenario .....	12
--	----

#### 10.1.2 Tabellenverzeichnis

Tabelle 1: Formale Aspekte.....	5
Tabelle 2: Liste der Autorinnen und Autoren.....	7
Tabelle 3: Geschäftsprozesse / Fachaufgaben.....	11
Tabelle 4: Anwendungen.....	13
Tabelle 5: IT-Systeme .....	14
Tabelle 6: Netze und Netzkomponenten.....	15
Tabelle 7: Gebäude und Räume.....	15
Tabelle 8: Modellierung der Bausteine .....	23
Tabelle 9: Anwendungshinweise .....	32
Tabelle 10: Glossar .....	36
Tabelle 11: Abkürzungen.....	37

### 10.2 Mitgeltende und referenzierte Dokumente

- [1] BSI-Standard 200-2 „IT-Grundschutz-Methodik“, V1.0
- [2] BSI-Standard 200-3 „Risikoanalyse auf der Basis von IT-Grundschutz“, V1.0
- [3] IT-Grundschutz-Kompendium, Edition 2023
- [4] IT-Grundschutz-Profil – Strukturbeschreibung, V1.0
- [5] BSI Technische Richtlinie 03138 Ersetzendes Scannen, V1.4.1
- [6] Regelungsdokument für das Informationssicherheitsmanagementsystem in der IT-Konsolidierung Bund
- [7] Vorläufiges Regelungsdokument 4.0 zum geplanten Mindeststandard für das ISMS ITKB
- [8] Hilfsdokument zur Risikoanalyse 230428\_FSK\_EAkteBund\_Risikoanalyse\_V1.xlsx
- [9] Kurzleitfaden Geschäftsprozessmanagement im Bundesministerium des Innern und für Heimat und seinen nachgeordneten Behörden, V1.1

## 10.3 Unterstützende Informationen

- (1) Zu einigen Bausteinen stellt das BSI unterstützende Umsetzungshinweise bereit:  
[https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompodium/Umsetzungshinweise/umsetzungshinweise\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompodium/Umsetzungshinweise/umsetzungshinweise_node.html)
- (2) Weitergehende Anforderungen an die eingesetzten Webbrowser enthält der Mindeststandard des BSI für Webbrowser:  
[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard Webbrowser V3 0.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard%20Webbrowser%20V3%200.pdf)
- (3) Musterdokumente und Arbeitshilfen zur Anwendung des IT-Grundschutzes befinden sich im „Werkzeugkasten der Sicherheitsberatung“ im internen Bereich der Website des BSI.

## 10.4 Glossar

Baustein	Das IT-Grundschutz-Kompodium enthält für unterschiedliche Vorgehensweisen, Komponenten und IT-Systeme Erläuterungen zur Gefährdungslage, Sicherheitsanforderungen und weiterführende Informationen, die jeweils in einem Baustein zusammengefasst sind.
Fachaufgabe	Als Fachaufgaben werden im IT-Grundschutz Geschäftsprozesse in Behörden bezeichnet.
Führungsprozess	Geschäftsprozess, der nicht der unmittelbaren Aufgabenerledigung dient, sondern strategische Zielsetzungen vorgibt und Rahmenbedingungen setzt, die sich auf die übrigen Prozessarten auswirken. Hierzu gehören u. a. Planung, Steuerung und Qualitätskontrolle.
Geschäftsprozess	Ein Geschäftsprozess ist eine Menge logisch verknüpfter Einzeltätigkeiten (Aufgaben, Arbeitsabläufe), die ausgeführt werden, um ein bestimmtes geschäftliches oder betriebliches Ziel zu erreichen.
Informationsverbund	Unter einem Informationsverbund ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Objekten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen.
Infrastruktur	Im IT-Grundschutz werden unter Infrastruktur die für die Informationsverarbeitung und die IT genutzten Gebäude und Räume, die Versorgungseinrichtungen, die Klimatisierung und die Verkabelung verstanden.
Institution	Mit dem Begriff Institution werden im IT-Grundschutz Unternehmen, Behörden und sonstige öffentliche oder private Organisationen bezeichnet.

Integrität	Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Informationen und der korrekten Funktionsweise von IT-Systemen.
IT-System	IT-Systeme sind technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden.
Kernprozess	Geschäftsprozess, der unmittelbar der Erfüllung der strategischen Zielsetzungen bzw. dem Zweck der Institution dient.
Kumulationseffekt	Der Kumulationseffekt beschreibt, dass sich der Schutzbedarf eines IT-Systems erhöhen kann, wenn durch Kumulation mehrerer (z. B. kleinerer) Schäden auf einem IT-System ein insgesamt höherer Gesamtschaden entstehen kann.
Maximumprinzip	Nach dem Maximumprinzip bestimmt der Schaden bzw. die Summe der Schäden mit den schwerwiegendsten Auswirkungen den Schutzbedarf eines Geschäftsprozesses, einer Anwendung bzw. eines IT-Systems.
Modellierung	Bei der Vorgehensweise nach IT-Grundschutz wird bei der Modellierung der betrachtete Informationsverbund einer Institution mit Hilfe der Bausteine aus dem IT-Grundschutz-Kompendium nachgebildet.
Schutzbedarf	Der Schutzbedarf beschreibt, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist.
Sicherheitsanforderung	Als Sicherheitsanforderung werden Anforderungen für den organisatorischen, personellen, infrastrukturellen und technischen Bereich bezeichnet, deren Erfüllung zur Erhöhung der Informationssicherheit notwendig ist bzw. dazu beiträgt.
Unterstützungsprozess	Geschäftsprozess, der eine Unterstützungsleistung für Kernprozesse erbringt und zum Beispiel Informationstechnik, Kommunikationsmittel oder Personal bereitstellt, aber selbst nur mittelbar einen Beitrag zur Zielerfüllung leistet.
Verfügbarkeit	Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendenden stets wie vorgesehen genutzt werden können.
Verteilungseffekt	Der Verteilungseffekt kann sich auf den Schutzbedarf relativierend auswirken, wenn zwar eine Anwendung einen hohen Schutzbedarf besitzt, ihn aber deshalb nicht auf ein betrachtetes IT-System überträgt, weil auf diesem IT-System nur unwesentliche Teilbereiche der Anwendung ausgeführt werden.

Vertraulichkeit	Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.
Zentrale Verwaltung	Organisationseinheit, die den allgemeinen Betrieb regelt und überwacht sowie alle Verwaltungsdienstleistungen plant, organisiert und durchführt.
Zielobjekt	Zielobjekte sind Teile des Informationsverbunds, denen im Rahmen der Modellierung ein oder mehrere Bausteine aus dem IT-Grundschutz-Kompendium zugeordnet werden können.

*Tabelle 10: Glossar*

## 10.5 Abkürzungen

BP	Betriebsplattform
BKB	Betriebskonsolidierung Bund
BSI	Bundesamt für Sicherheit in der Informationstechnik
DMS	Dokumentenmanagementsystem
DSB	Datenschutzbeauftragte
FM	Facility Management
GSB	Geheimschutzbeauftragte
GVP	Geschäftsverteilungsplan
ISB	Informationssicherheitsbeauftragte
ISMS	Informationssicherheitsmanagementsystem
ITKB	IT-Konsolidierung des Bundes
ITZ	Informationstechnikzentrum
NdB	Netze des Bundes
NFB	Notfallbeauftragte (BCM-Beauftragte)
SINA	Sichere Inter-Netzwerk Architektur
SLA	Service Level Agreement
VPN	Virtuelles Privates Netz
WAN	Wide Area Network
WLAN	Wireless Local Area Network

Tabelle 11: Abkürzungen