

# **IT-Grundschutz-Profil für Bundesgerichte**

Version:	1.0
Revisionszyklus:	2-jährig
Version IT-Grundschutz-Kompendium	2023

# Inhaltsverzeichnis

1	Einleitung.....	1
2	Formale Aspekte .....	2
3	Haftungsausschluss.....	2
4	Liste der Autorinnen und Autoren .....	2
5	Management Summary.....	2
5.1	Zielgruppe .....	2
5.2	Zielsetzung .....	3
6	Festlegung des Geltungsbereichs.....	3
6.1	Zielgruppe .....	3
6.2	Beschreibung des Schutzbedarfs .....	3
6.3	IT-Grundschutz Vorgehensweise .....	3
6.4	Kompatibilität zu anderen Standards .....	4
6.5	Berücksichtigte Rahmenbedingungen.....	4
7	Abgrenzung des Informationsverbundes .....	4
7.1	Bestandteile des Informationsverbundes.....	4
7.2	Nicht berücksichtigte Teile.....	4
8	Referenzarchitektur .....	6
8.1	Geschäftsprozesse / Fachaufgaben.....	6
8.2	Anwendungen.....	9
8.3	IT-Systeme.....	10
8.4	Netze und Netzkomponenten .....	10
8.5	Gebäude und Räume .....	11
8.6	Netzplan.....	12
8.7	Umgang mit Abweichungen.....	12
9	Zu erfüllende Anforderungen und umzusetzende Maßnahmen.....	13
9.1	Feststellung des Schutzbedarfs.....	13
9.2	Schutzbedarfsfeststellung für Geschäftsprozesse / Fachaufgaben .....	13
9.3	Schutzbedarfsfeststellung für Anwendungen .....	15
9.4	Schutzbedarfsfeststellung für IT-Systeme .....	16
9.5	Schutzbedarfsfeststellung für Netze und Netzkomponenten.....	16
9.6	Schutzbedarfsfeststellung für Gebäude und Räume.....	17
10	Zuordnung der relevanten Bausteine .....	17
10.1	Modellierung.....	17
10.2	Relevanz der Anforderungen .....	21
11	Restrisiko.....	22
12	Unterstützende Informationen .....	22

# Versionshistorie

Datum	Version	Änderung	Bearbeiter
07.03.2023	1.0	Fertigstellung Version 1.0	siehe Liste der Autoren

# 1 Einleitung

Der IT-Grundschutz des BSI ist eine seit Jahren bewährte Methodik zum Aufbau eines Managementsystems für Informationssicherheit (ISMS), um das Niveau der Informationssicherheit in Institutionen jeder Größenordnung zu erhöhen.

Für einen erleichterten Einstieg in den Informationssicherheitsprozess ist das vorliegende IT-Grundschutz-Profil erstellt worden. Ein IT-Grundschutz-Profil ist ein Muster-Sicherheitskonzept, das als Schablone für Institutionen mit vergleichbaren Rahmenbedingungen dient. Schritte, die nach IT-Grundschutz zu gehen sind, sind in diesem Muster pauschalisiert. So ist es schließlich allen Interessierten in vergleichbaren Institutionen möglich, mit Hilfe der Schablone die Informationssicherheit in der jeweiligen Einrichtung zu erhöhen.

Das IT-Grundschutz-Profil für Bundesgerichte richtet sich an die für Informationssicherheit verantwortlichen Entscheidungsträger aus dem Bereich der Justiz.

Dieses IT-Grundschutz-Profil soll den Anwendern helfen, einen Informationssicherheitsprozess in einem Gericht zu installieren und diesen an deren Bedürfnisse anzupassen. Es soll als Schablone dienen, den IT-Grundschutz des BSI in geeigneter Weise zu implementieren.

Im Rahmen eines Projektes des BSI zur Neupositionierung des IT-Grundschutzes in der Bundesverwaltung wurde die Erstellung geeigneter IT-Grundschutzprofile als Arbeitshilfen angeregt und in Kooperation mit Informationssicherheitsbeauftragten der Bundesgerichte und dem BSI gemeinsam erarbeitet. Es soll sowohl Bundesgerichten als auch beispielsweise vergleichbaren Gerichten auf Landesebene als Grundlage für die Erstellung eines eigenen Sicherheitskonzeptes dienen.

Das vorliegende Dokument „IT-Grundschutz-Profil für Bundesgerichte“ umfasst ausgehend von den als relevant betrachteten Geschäftsprozessen:

- eine Liste der relevanten Zielobjekte (Anwendungen, IT-Systeme sowie Räumlichkeiten), die es zu schützen gilt,
- eine Zuordnung der dazu passenden IT-Grundschutz-Bausteine mit Anforderungen und Umsetzungshinweisen sowie
- Empfehlungen zur Umsetzungsreihenfolge.

## 2 Formale Aspekte

Aspekt	Beschreibung
Titel:	IT-Grundschutz-Profil für Bundesgerichte
Ansprechpartner:	siehe Liste der Autoren
Version:	1.0
IT-Grundschutz-Kompendium:	Edition 2023
Revisionszyklus:	2-jährig
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
Herr Martin Bierhoff	Bundesarbeitsgericht
Herr Holger Dittrich	Bundesarbeitsgericht
Herr Jan Koldas	Bundesgerichtshof
Herr Gerd Sarnes	Bundesgerichtshof
Herr Matthias Schüller	Bundespatentgericht
Herr Andreas Schantin	Bundesverfassungsgericht
Herr Jan Stowasser	Bundesverwaltungsgericht
Herr Birger Klein	Bundesamt für Sicherheit in der Informationstechnik
Frau Claudia Gola	Bundesamt für Sicherheit in der Informationstechnik

*Tabelle 2: Liste der Autorinnen und Autoren.*

## 5 Management Summary

### 5.1 Zielgruppe

Dieses IT-Grundschutz-Profil richtet sich an die für die Informationssicherheit zuständigen Stellen der Bundesgerichte und vergleichbarer Gerichte. Für Bundesgerichte sind dies insbesondere die gemäß UP Bund zu bestellenden IT-Sicherheitsbeauftragten bzw.

Informationssicherheitsbeauftragten sowie weitere im Rahmen eines Informationssicherheitsprozesses in der Verantwortung stehende Entscheidungsträger.

## **5.2 Zielsetzung**

Dieses IT-Grundschutz-Profil soll helfen, den Ablauf eines Gerichtsverfahrens, unter Anwendung der Standards des BSI, soweit diese einschlägig sind, abzusichern. Beachtung findet insbesondere § 8 Abs. 1 BSI-Gesetz (BSIG) i.V.m. § 2 Abs. 3 BSIG. Die folgenden Ausführungen zur Darstellung und Bewertung aller Geschäftsprozesse, die ab Beginn bis zum Ende eines Gerichtsverfahrens zutreffend sind, definieren ein empfohlenes Mindest-Schutzniveau für die Informationssicherheit eines Gerichtsverfahrens. Das IT-Grundschutz-Profil für Bundesgerichte soll als Vorlage verstanden werden und kann für gegebenenfalls abweichend etablierte Geschäftsprozesse individuell angepasst werden. Handlungsbedarf ergibt sich unter Umständen für die Strafgerichtsbarkeit. Gleichwohl besteht, unter Einbeziehung bereits vorliegender Dokumente, wie zum Beispiel das Datenschutzkonzept für die elektronische Aktenbearbeitung mit der Software VIS-Justiz beim Bundespatentgericht oder eines generischen Sicherheitskonzepts für das Fachsystem Goša oder vergleichbarer Dokumente zu weiteren in den Bundesgerichten eingesetzten IT-Systemen, die Möglichkeit zur Partizipation. Eine Liste etwaiger Dokumente ist im Kapitel 12 Unterstützende Informationen aufgeführt.

# **6 Festlegung des Geltungsbereichs**

## **6.1 Zielgruppe**

Das IT-Grundschutz-Profil für Bundesgerichte richtet sich an die für Informationssicherheit verantwortlichen Entscheidungsträger von Bundesgerichten und vergleichbaren Gerichten.

## **6.2 Beschreibung des Schutzbedarfs**

Der Schutzbedarf kann in den Gerichten variieren, i.d.R. wird jedoch von einem Schutzbedarf auf dem Niveau "Normal" ausgegangen. In der Schutzbedarfsfeststellung werden dann Kriterien benannt, die zu einer Erhöhung des Schutzbedarfs führen können und bei der Ableitung eines Sicherheitskonzeptes aus dem Profil individuell betrachtet werden sollten.

Der Sammel-Geschäftsprozess Basis-IT "erbt" den maximalen Schutzbedarf aus den anderen Geschäftsprozessen.

Infolgedessen wird in diesem IT-Grundschutz-Profil ein Schutzniveau mit mindestens der Standard-Absicherung der IT-Grundschutz-Vorgehensweise angestrebt.

## **6.3 IT-Grundschutz Vorgehensweise**

Der IT-Grundschutz des BSI bietet die Vorgehensweisen Basis-, Standard oder Kern-Absicherung an. Abhängig von der gewählten Vorgehensweise müssen die in den Bausteinen beschriebenen Anforderungen umgesetzt werden. Die beschriebenen Anforderungen in diesem IT-Grundschutz-Profil entsprechen mindestens der Standard-Absicherung des BSI-Standards 200-2.

## **6.4 Kompatibilität zu anderen Standards**

Durch eine Umsetzung der Standard-Absicherung besteht Kompatibilität zu ISO 27001.

## **6.5 Berücksichtigte Rahmenbedingungen**

Vorgaben aus der DSGVO, dem BSI-Gesetz und dem UP Bund werden in diesem IT-Grundschutz-Profil berücksichtigt.

# **7 Abgrenzung des Informationsverbundes**

Der Geltungsbereich einer Sicherheitskonzeption nach BSI-Standard 200-2 wird als Informationsverbund bezeichnet. Die Referenzarchitektur dieses Grundschutzprofils enthält die Geschäftsprozesse, die hinsichtlich der gesetzlichen Aufgabenerfüllung bei Bundesgerichten im Bereich der Rechtsprechung relevant sind (siehe 8.1).

## **7.1 Bestandteile des Informationsverbundes**

Der Informationsverbund des Grundschutzprofils beschränkt sich auf gesetzlichen Kernaufgaben der Rechtsprechung, die durch die Bundesgerichte ausgeübt wird. Er enthält nur die für diese Aufgaben wesentlichen Geschäftsprozesse.

Die betrachteten Geschäftsprozesse orientieren sich am Lauf eines Verfahrens vom Eingang eines Verfahrensanspruchs bis zur Entscheidung und deren Veröffentlichung. Kernaufgaben der Rechtsprechung werden dabei von den aus Richterinnen und Richtern bestehenden Spruchkörpern wahrgenommen. Darüber hinaus sind Gerichts- beziehungsweise Justizverwaltungen an den für die Durchführung der Verfahren notwendigen Geschäftsprozessen beteiligt. Dazu zählen auch Serviceeinheiten wie Posteingangsstellen und Registraturen.

Der Informationsverbund muss alle Geschäftsprozesse beinhalten, die für den Ablauf eines Verfahrens unmittelbar erforderlich sind. Abschnitt 8.1 führt wesentliche Geschäftsprozesse als Teil der Referenzarchitektur auf. Anwender dieses Grundschutzprofils müssen prüfen, ob alle für sie relevanten Aspekte in der Referenzarchitektur abgebildet sind. Existieren weitere, für den Kernbereich essenzielle Geschäftsprozesse, sind diese in Informationsverbund aufzunehmen.

Der Informationsverbund beinhaltet alle Anwendungen und Systeme, die für die ordnungsgemäße Ausführung der Geschäftsprozesse erforderlich sind. Ferner sind Basis- und Querschnittsdienste berücksichtigt, die für die Informationssicherheit von wesentlicher Bedeutung sind (z. B. Authentisierungsdienste, Datensicherung). Übergreifende Aspekte der Informationssicherheit des Informationsverbunds, die nicht unmittelbar den Geschäftsprozessen zuordnen sind, werden durch die Prozess-Bausteine des IT-Grundschutzkompendiums modelliert und berücksichtigt.

## **7.2 Nicht berücksichtigte Teile**

An Gerichten nehmen weitere Organisationseinheiten Aufgaben wahr, die nicht unmittelbar der Rechtsprechung zuzuordnen sind. Diese werden im Grundschutzprofil nicht betrachtet. Insbesondere sind die Aufgaben der an Gerichten eingerichteten Dokumentationsstellen,

Bibliotheken und die allgemeinen Verwaltungen nicht im vollen Umfang im Grundsatzprofil berücksichtigt.

Der Informationsverbund umfasst auch solche Geschäftsprozesse, Anwendungen und Systeme eines Gerichts nicht, in denen zwar potenziell Informationen mit erhöhtem Schutzbedarf verarbeitet werden, die aber nicht der Kernbereich der Rechtsprechung zuzuordnen sind (z. B. Prozesse, Anwendungen und Systeme der Personalabteilungen).



## 8 Referenzarchitektur

### 8.1 Geschäftsprozesse / Fachaufgaben

ID	Geschäftsprozesse / Fachaufgaben	Beschreibung
GP01	Posteingang / Zuteilung	<p>Eingang von Rechtsmitteln in digitaler und Papierform oder per FAX:</p> <p>Der Posteingang bei den Gerichten erfolgt überwiegend in digitaler Form. Seit 2018 sind gesetzliche Regelungen für die elektronische Kommunikation mit den Gerichten in Kraft getreten, die u.a. die Nutzung der EGVP-Infrastruktur zum Gegenstand haben. Seit dem 1. Januar 2022 sind Rechtsanwälte, Behörden und juristische Personen des öffentlichen Rechts zur Nutzung dieses Kommunikationswegs verpflichtet. Durch Größenbeschränkungen bei der Übermittlung sind aber auch noch DVD und CD als physische Datenträger erlaubt.</p> <p>Ausnahmen bestehen derzeit noch für Patentanwälte, Steuerberater und Wirtschaftsprüfer. Hier können die Rechtsmittel weiterhin per Brief, FAX oder eigens eingerichteter elektronischer Poststellen eingereicht werden. Bürger und Organisationen dürfen ihre Eingaben auch weiterhin über ein DE-Mail-Konto versenden. Das Bundesverfassungsgericht nimmt bisher nicht am EGVP teil. Der Eingang erfolgt ausschließlich in Papierform.</p>
GP02	Scan-Stelle	<p>Digitalisierung von Posteingang und Bestandsakten:</p> <p>Die Scan-Stellen übernehmen die Digitalisierung des analogen Posteingangs. Dabei ist das „Ersetzende Scannen“ nach der Technischen Richtlinie BSI TR-03138 (TR-RESISCAN) anzuwenden. Zusätzlich können auch die bereits vorhandenen Bestandsakten digitalisiert und in die elektronische Akte überführt werden.</p>

ID	Geschäftsprozesse / Fachaufgaben	Beschreibung
GP03	Erfassung	<p>Verfahren anlegen, soweit noch nicht geschehen, Verfahren bearbeiten, Metadaten erfassen:</p> <p>Die eingegangenen Medien werden vereinnahmt und in der elektronischen Akte abgelegt. Für neue Verfahren wird ein Aktenzeichen gebildet, zusätzliche Medien werden zu einem bereits bestehenden Verfahren hinzugefügt.</p> <p>Historisch bedingt verwenden die meisten Gerichte eine zusätzliche Fachanwendung für die Vorgangsverfolgung, Anreicherung mit Metadaten und Schriftguterstellung, da die frühen Versionen der elektronischen Akten diese Funktionen noch nicht bereitstellen konnten.</p>
GP04	Geschäftsstellen- Bearbeitung	<p>Vorgänge prüfen, Fristen setzen, Gebühren festlegen und Endbearbeitung:</p> <p>Die Vorgänge werden den Geschäftsstellen der Senate nach deren Zuständigkeit zugewiesen. Die Geschäftsstelle prüft die zugewiesenen Unterlagen, setzt Fristen für die Bearbeitung und informiert die beteiligten Parteien. Nach der Urteilsfindung werden hier auch die Gebühren für die Parteien festgelegt, Schriftstücke gefertigt und eine Endbearbeitung des Verfahrens durchgeführt.</p>
GP05	Votum / Beratung	<p>Vorbereitung des Votums, Übergabe zur Beratung:</p> <p>Die vorliegenden Sachverhalte werden von einer RichterIn / einem Richter zusammengefasst und bewertet. Am Ende steht ein Entscheidungsvorschlag/Votum für das Verfahren. Die anschließende Beratung der Richterinnen und Richter zu einem Verfahren erfolgt untereinander in nichtöffentlicher Sitzung. Der Austausch darin ist im höchsten Maße schützenswert. Informationen dazu oder gar Inhalte aus der Beratung dürfen nicht vorab oder im Nachgang an die Öffentlichkeit gelangen.</p>

ID	Geschäftsprozesse / Fachaufgaben	Beschreibung
GP06	Verhandlung	Mündliche Verhandlung mit Verfahrensbeteiligten: Kommt es zu einer mündlichen Verhandlung, werden die Verfahrensbeteiligten vor Gericht geladen. Die Verhandlung erfolgt in der Regel am Gericht öffentlich, außer in Strafsachen und wenn andere Gründe eine nichtöffentliche Verhandlung erfordern. Inzwischen kann eine Verhandlung auch mittels Videokonferenz durchgeführt werden. Verfahren können jedoch auch ohne eine mündliche Verhandlung abgeschlossen werden.
GP07	Urteil	Erstellung und Verkündung des Urteils: Nach der Urteilsfindung wird das schriftliche Urteil durch die Geschäftsstellen erstellt und zuerst den Verfahrensbeteiligten zugestellt oder in einem weiteren Termin verkündet.
GP08	Urteil veröffentlichen	Anonymisierung des Urteils und Pressemitteilung: Vor der abschließenden Veröffentlichung des Urteils müssen darin enthaltene personenbezogene Daten anonymisiert werden. Erst dann kann der Inhalt auf der Webseite des Gerichts / in einer Datenbank eingestellt und eine Pressemitteilung darüber herausgegeben werden.
GP09	Basis-IT	Sammelprozess für die Nutzung von Clients, Druckern, Telefonen: Die Basis-IT ist eine unterstützende Fachaufgabe, die von allen anderen Aufgaben verwendet wird. Unter dem Begriff wird die IT-Infrastruktur, Ausstattung der Arbeitsplätze mit Client-Computer und Basis-Software, Drucker und Telefon zusammengefasst.

*Tabelle 3: Geschäftsprozesse / Fachaufgaben (Stand: 23.08.2022)*

## 8.2 Anwendungen

ID	Anwendungen	Zuordnung zu Prozesse
A01	EGVP (Elektronisches Gerichts-Verwaltungspostfach EGVP)	GP01, GP07
A02	Fax-Dienst	GP01
A03	eAkte	GP01, GP02, GP03, GP04, GP05, GP06, GP07
A04	Scan-Dienst	GP02
A05	Fachanwendung für Metadaten und Schriftgut Erstellung	GP03, GP04, GP07
A06	Digitale Recherche ( <i>Juris - Outsourcing</i> )	GP05
A07	Internes Videokonferenzsystem	GP05
A08	Externes Videokonferenzsystem	GP06
A09	Web-Auftritt	GP08
A10	Office, E-Mail	GP09
A11	VoIP	GP09
A12	eAkte Client Software	GP09
A13	EGVP Client Software	GP09
A14	Client für Fachanwendung für Metadaten und Schriftgut Erstellung	GP09
A15	Verzeichnis-Dienst	GP09
A16	Backup	GP09
A17	Storage	GP09
A18	Virtualisierungsplattform	GP09

*Tabelle 4: Anwendungen*

### 8.3 IT-Systeme

ID	IT-Systeme	Zuordnung zu Anwendungen
S01	EGVP-Server Win/Linux	A01
S02	Fax-Server	A02
S03	eAkte Application Server Win/Linux	A03
S04	eAkte Datenbankserver Win/Linux	A03
S05	Scan-Server Win/Linux	A04
C02	Scan-Client Win	A04
S07	Application Server Win/Linux	A05
S08	Datenbank Server Win/Linux	A05
S09	Videokonferenz-Application Server Win/Linux	A07
S10	Videokonferenz-Application Server Win/Linux	A08
S11	Web-Server	A09
C01	Client Win-10 Desktop/Notebook	A10, A11, A12, A13, A14
S12	Telefon	-
S13	Drucker	-
S14	Smartphones (Android/iOS)	-
S15	Tablet (Android/iOS)	-
S16	Telefonanlage	-
S17	Arbeitsplatz-Drucker	-
S18	Server für Verzeichnisdienst	A15
S19	Server für Backup	A16
S20	Storage-System	A17
S21	Virtualisierungsserver	A18
S22	Scanner der Scanstelle	A04

Tabelle 5: IT-Systeme

### 8.4 Netze und Netzkomponenten

ID	Netze und Netzkomponenten	Zuordnung IT-Systeme
NET	Netze (Router, Switch, Firewall)	-

Tabelle 6: Netze und Netzkomponenten

## 8.5 Gebäude und Räume

ID	Gebäude oder Raum	Zuordnung zu IT-Systemen / Netzkomponenten
G1	Gebäude 1 mit R1, R2, R3, R4, R6, R7	
R1	Serverraum	S01, S03, S04, S05, S07, S08, S09, S10, S11, S18, S19, S20, S21
R2	TK-Raum	S02, S16
R3	Scan-Stelle	C02, S22
R4	Bürraum	C01, S12, S17
R5	mobiles Arbeiten	C01, S14, S15
R6	Flur	S13
R7	Sitzungssaal	S10

*Tabelle 7: Gebäude und Räume*

## 8.6 Netzplan

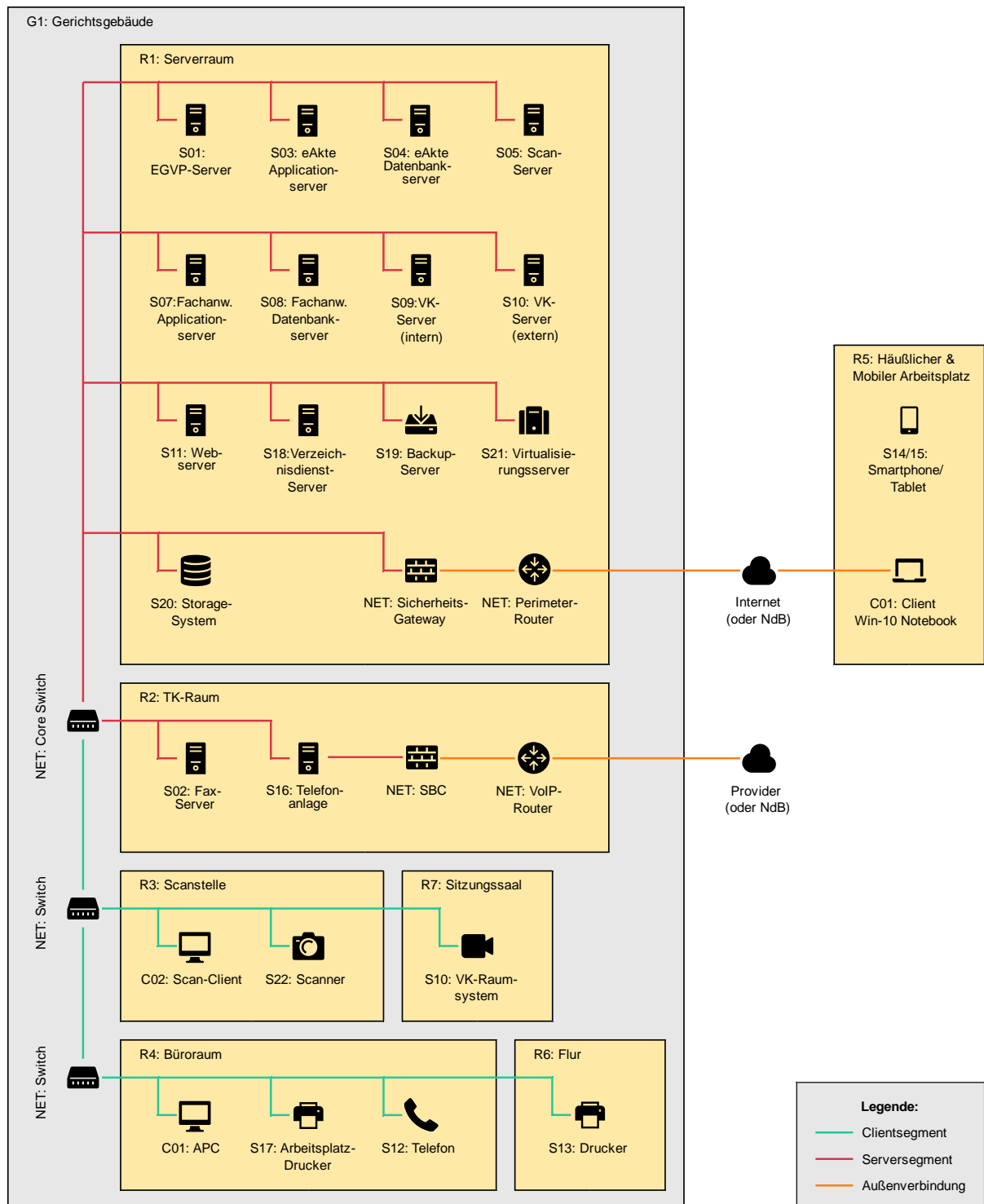


Abbildung 1: Netzplan (Stand: Version 0.6 vom 26.10.2022)

## 8.7 Umgang mit Abweichungen

Weicht der zu schützende Informationsverbund von der Referenzarchitektur ab, sind die zusätzlichen oder nicht vorhandenen Objekte zu dokumentieren. Diesen Objekten sind geeignete

Bausteine des IT-Grundschutz-Kompodiums zuzuordnen. Die aus den Bausteinen abgeleiteten Anforderungen müssen in Abhängigkeit des Schutzbedarfs angepasst werden.

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

Das IT-Grundschutz-Kompodium ist die grundlegende Veröffentlichung des IT-Grundschutzes. Im Fokus des IT-Grundschutz-Kompodiums stehen die sogenannten IT-Grundschutz-Bausteine. In den IT-Grundschutz-Bausteinen werden jeweils zu einem Thema alle relevanten Sicherheitsaspekte beleuchtet und Sicherheitsanforderungen zur Absicherung gegeben.

In einem IT-Grundschutz-Profil kann vorgegeben werden, ob alle Anforderungen eines Bausteins oder lediglich eine Auswahl relevant sind. Außerdem können und sollten die ausgewählten Anforderungen konkretisiert werden. Nicht nur vorhandene Anforderungen aus den IT-Grundschutz-Bausteinen können dem IT-Grundschutz-Profil zugeordnet werden, sondern auch bisher im IT-Grundschutz noch nicht vorhandene Anforderungen. Auf diese Weise kann mit Hilfe der IT-Grundschutz-Profile ein Sicherheitsniveau erreicht werden, das exakt dem Schutzbedarf des betrachteten Anwendungsbereiches entspricht.

Hierzu ist zunächst der Schutzbedarf der Geschäftsprozesse / Fachaufgaben, Anwendungen, IT-Systeme und Kommunikationsverbindungen festzulegen. Anschließend müssen die relevanten Bausteine identifiziert und ggf. eine Anpassung der Anforderungen an die entsprechende Zielgruppe durchgeführt werden.

### **9.1 Feststellung des Schutzbedarfs**

Ziel der Schutzbedarfsfeststellung ist es, für die erfassten Objekte im Geltungsbereich zu entscheiden, welchen Schutzbedarf sie bezüglich Vertraulichkeit, Integrität und Verfügbarkeit besitzen. Dieser Schutzbedarf orientiert sich an den möglichen Schäden, die eintreten können. Die Grundlage zur Bestimmung des Schutzbedarfs verschiedener Objekte ist der Schutzbedarf der Geschäftsprozesse und der zugehörigen Informationen. Der für diese Elemente ermittelte Schutzbedarf vererbt sich auf die für deren Verarbeitung genutzten Objekte, also Anwendungen, IT-Systeme, Gebäude und Räume und Kommunikationsverbindungen. Das Vorgehen ist im Detail im BSI-Standard 200-2 beschrieben. Wenn nicht anders angegeben, werden in diesem IT-Grundschutz-Profil die Schadensszenarien und Schutzbedarfskategorien aus dem BSI-Standard 200-2 verwendet.

### **9.2 Schutzbedarfsfeststellung für Geschäftsprozesse / Fachaufgaben**

Zur Bestimmung des Schutzbedarfs wird im Rahmen dieses IT-Grundschutzprofils der Schutzbedarf auf Ebene der Geschäftsprozesse definiert und auf die nachfolgenden Zielobjekte nach Maximalprinzip vererbt.

Bei der Ableitung eines Sicherheitskonzeptes aus dem IT-Grundschutzprofil sollten sowohl die Schutzbedarfe der Geschäftsprozesse als auch deren Vererbung auf die zugeordneten Zielobjekte noch einmal individuell betrachtet werden.



ID	Schutzbedarf (Vertraulichkeit/Integrität/Verfügbarkeit)	Begründung
GP01	normal/normal/normal	<p>Integrität: es muss nachvollziehbar sein, wer was wann eingereicht hat, daher erhöhter Schutzbedarf möglich. Führen nicht festgestellte Fehler im Postfach (Anträge) zu Rechtsfolgen, die nicht heilbar sind?</p> <p>Kriterien, die Schutzbedarf erhöhen können:</p> <ul style="list-style-type: none"> <li>• Vertraulichkeit: besondere personenbezogene Daten/Kategorien, Sozialgeheimnis, Steuergeheimnis, Verschlusssachen</li> <li>• Integrität: nicht heilbare Rechtsfolgen von Fehlern in den Anträgen</li> <li>• Verfügbarkeit: bei Eilanträgen kann es zeitkritische Verfahren geben, die einen erhöhten Schutzbedarf erfordern</li> </ul>
GP02	normal/normal/normal	<p>Wie GP01</p> <p>Kriterien, die Schutzbedarf erhöhen können: -/-</p>
GP03	normal/normal/normal	<p>Wie GP01</p> <p>Kriterien, die Schutzbedarf erhöhen können: -/-</p>
GP04	normal/normal/normal	<p>Wie GP01</p> <p>Kriterien, die Schutzbedarf erhöhen können: -/-</p>
GP05	hoch/normal/hoch	<p>Votum hat erhöhte Vertraulichkeit</p> <p>Bei der Beratung und Verhandlung ist ggf. erhöhte Verfügbarkeit erforderlich</p> <p>Kriterien, die Schutzbedarf erhöhen können:</p> <ul style="list-style-type: none"> <li>• Abstimmungsgeheimnis</li> </ul>
GP06	normal/normal/normal	<p>Vertraulichkeit öffentlicher Verhandlung normal</p> <p>Bei nicht öffentlichen Verhandlungen (Strafsachen) erhöhter Schutzbedarf für Vertraulichkeit.</p> <p>Bei der Beratung und Verhandlung ist ggf. erhöhte Verfügbarkeit erforderlich (Eilverfahren).</p> <p>Kriterien, die Schutzbedarf erhöhen können:</p> <ul style="list-style-type: none"> <li>• Vertraulichkeit: Strafsachen, Jugendschutz, Sozialgeheimnis, Steuergeheimnis</li> <li>• Verfügbarkeit: Eilverfahren</li> </ul>
GP07	normal/normal/normal	<p>Wie GP06</p> <p>Kriterien, die Schutzbedarf erhöhen können:</p> <ul style="list-style-type: none"> <li>• Nicht veröffentlichte Urteile können erhöhten Schutzbedarf für Vertraulichkeit haben.</li> </ul>

GP08	normal/normal/normal	Wie GP06 Kriterien, die Schutzbedarf erhöhen können: -/-
GP09	hoch/normal/hoch	GP09 „erbt“ höchsten Schutzbedarf aus allen anderen Geschäftsprozessen Kriterien, die Schutzbedarf erhöhen können: -/-

*Tabelle 8: Schutzbedarfsfeststellung für Geschäftsprozesse / Fachaufgaben*

### 9.3 Schutzbedarfsfeststellung für Anwendungen

ID	Schutzbedarf (Vertraulichkeit/Integrität/Verfügbarkeit)	Begründung
A01	normal/normal/hoch	Vererbung nach Maximumprinzip
A02	normal/normal/normal	Vererbung nach Maximumprinzip
A03	hoch/normal/hoch	Vererbung nach Maximumprinzip
A04	normal/normal/normal	Vererbung nach Maximumprinzip
A05	normal/normal/normal	Vererbung nach Maximumprinzip
A06	hoch/normal/hoch	Vererbung nach Maximumprinzip
A07	hoch/normal/hoch	Vererbung nach Maximumprinzip
A08	normal/normal/normal	Vererbung nach Maximumprinzip
A09	normal/normal/normal	Vererbung nach Maximumprinzip
A10	hoch/normal/hoch	Vererbung nach Maximumprinzip
A11	hoch/normal/hoch	Vererbung nach Maximumprinzip
A12	hoch/normal/hoch	Vererbung nach Maximumprinzip
A13	hoch/normal/hoch	Vererbung nach Maximumprinzip
A14	hoch/normal/hoch	Vererbung nach Maximumprinzip
A15	hoch/normal/hoch	Vererbung nach Maximumprinzip
A16	hoch/normal/hoch	Vererbung nach Maximumprinzip
A17	hoch/normal/hoch	Vererbung nach Maximumprinzip
A18	hoch/normal/hoch	Vererbung nach Maximumprinzip

*Tabelle 9: Schutzbedarfsfeststellung für Anwendungen*

## 9.4 Schutzbedarfsfeststellung für IT-Systeme

ID	Schutzbedarf (Vertraulichkeit/Integrität/Verfügbarkeit)	Begründung
S01	normal/normal/normal	Vererbung nach Maximumprinzip
S02	normal/normal/normal	Vererbung nach Maximumprinzip
S03	hoch/normal/hoch	Vererbung nach Maximumprinzip
S04	hoch/normal/hoch	Vererbung nach Maximumprinzip
S05	normal/normal/normal	Vererbung nach Maximumprinzip
S07	normal/normal/normal	Vererbung nach Maximumprinzip
S08	normal/normal/normal	Vererbung nach Maximumprinzip
S09	hoch/normal/hoch	Vererbung nach Maximumprinzip
S10	normal/normal/normal	Vererbung nach Maximumprinzip
S11	normal/normal/normal	Vererbung nach Maximumprinzip
S12	hoch/normal/hoch	Vererbung nach Maximumprinzip
S13	hoch/normal/hoch	Vererbung nach Maximumprinzip
S14	hoch/normal/hoch	Vererbung nach Maximumprinzip
S15	hoch/normal/hoch	Vererbung nach Maximumprinzip
S16	hoch/normal/hoch	Vererbung nach Maximumprinzip
S17	hoch/normal/hoch	Vererbung nach Maximumprinzip
S18	hoch/normal/hoch	Vererbung nach Maximumprinzip
S19	hoch/normal/hoch	Vererbung nach Maximumprinzip
S20	hoch/normal/hoch	Vererbung nach Maximumprinzip
S21	hoch/normal/hoch	Vererbung nach Maximumprinzip
S22	hoch/normal/hoch	Vererbung nach Maximumprinzip
C01	hoch/normal/hoch	Vererbung nach Maximumprinzip
C02	normal/normal/normal	Vererbung nach Maximumprinzip

Tabelle 10: Schutzbedarfsfeststellung für IT-Systeme

## 9.5 Schutzbedarfsfeststellung für Netze und Netzkomponenten

ID	Schutzbedarf (Vertraulichkeit/Integrität/Verfügbarkeit)	Begründung
NET	hoch/normal/hoch	Vererbung nach Maximumprinzip

Tabelle 11: Schutzbedarfsfeststellung für Netz und Netzkomponenten

## 9.6 Schutzbedarfsfeststellung für Gebäude und Räume

ID	Schutzbedarf (Vertraulichkeit/Integrität/Verfügbarkeit)	Begründung
G1	hoch/normal/hoch	Vererbung nach Maximumprinzip
R1	hoch/normal/hoch	Vererbung nach Maximumprinzip
R2	hoch/normal/hoch	Vererbung nach Maximumprinzip
R3	hoch/normal/hoch	Vererbung nach Maximumprinzip
R4	hoch/normal/hoch	Vererbung nach Maximumprinzip
R5	hoch/normal/hoch	Vererbung nach Maximumprinzip
R6	hoch/normal/hoch	Vererbung nach Maximumprinzip

Tabelle 12: Schutzbedarfsfeststellung für Gebäude und Räume

## 10 Zuordnung der relevanten Bausteine

Nachdem die Referenzarchitektur mit den entsprechenden Zielobjekte definiert ist und die Schutzbedarfsfeststellung durchgeführt wurde, besteht die nächste Aufgabe darin, den betrachteten Informationsverbund (Untersuchungsgegenstand) mit Hilfe des IT-Grundschutz-Modells nachzubilden. Dafür werden im IT-Grundschutz-Kompendium vorhandene Bausteine ausgewählt (siehe auch BSI-Standard 200-2, Kapitel 8.3 Modellierung eines Informationsverbunds oder Kapitel 2 des IT-Grundschutz-Kompendiums).

### 10.1 Modellierung

Baustein	Zielobjekte
ISMS.1 Sicherheitsmanagement	Informationsverbund/übergeordnete Aspekte
ORP.1 Organisation	Informationsverbund/übergeordnete Aspekte
ORP.2 Personal	Informationsverbund/übergeordnete Aspekte
ORP.3 Sensibilisierung und Schulung zur Informationssicherheit	Informationsverbund/übergeordnete Aspekte
ORP.4 Identitäts- und Berechtigungsmanagement	Informationsverbund/übergeordnete Aspekte
ORP.5 Compliance Management (Anforderungsmanagement)	Informationsverbund/übergeordnete Aspekte
CON.1 Kryptokonzept	Informationsverbund/übergeordnete Aspekte
CON.2 Datenschutz	Informationsverbund/übergeordnete Aspekte
CON.3 Datensicherungskonzept	Informationsverbund/übergeordnete Aspekte
CON.6 Löschen und Vernichten	Informationsverbund/übergeordnete Aspekte
CON.7 Informationssicherheit auf Auslandsreisen	Informationsverbund/übergeordnete Aspekte
CON.8 Software-Entwicklung	nicht relevant
CON.9 Informationsaustausch	Informationsverbund/übergeordnete Aspekte

Baustein	Zielobjekte
CON.10 Entwicklung von Webanwendungen	nicht relevant
CON.11.1 Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)	Informationsverbund/übergeordnete Aspekte
OPS.1.1.1 Allgemeiner IT-Betrieb	Informationsverbund/übergeordnete Aspekte
OPS.1.1.2 Ordnungsgemäße IT-Administration	Informationsverbund/übergeordnete Aspekte
OPS.1.1.3 Patch- und Änderungsmanagement	Informationsverbund/übergeordnete Aspekte
OPS.1.1.4 Schutz vor Schadprogrammen	Informationsverbund/übergeordnete Aspekte
OPS.1.1.5 Protokollierung	Informationsverbund/übergeordnete Aspekte
OPS.1.1.6 Software-Tests und -Freigaben	Informationsverbund/übergeordnete Aspekte
OPS.1.1.7 Systemmanagement	nicht relevant
OPS.1.2.2 Archivierung	Informationsverbund/übergeordnete Aspekte
OPS.1.2.4 Telearbeit	R5
OPS.1.2.5 Fernwartung	Informationsverbund/übergeordnete Aspekte
OPS.1.2.6 NTP -Zeitsynchronisation	S18
OPS.2.3 Nutzung von Outsourcing	A06 (Dienstleister)
OPS.2.2 Cloud-Nutzung	A08
OPS.3.2 Anbieten von Outsourcing	nicht relevant
DER.1 Detektion von sicherheitsrelevanten Ereignissen	Informationsverbund/übergeordnete Aspekte
DER.2.1 Behandlung von Sicherheitsvorfällen	Informationsverbund/übergeordnete Aspekte
DER.2.2 Vorsorge für die IT-Forensik	Informationsverbund/übergeordnete Aspekte
DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle	Informationsverbund/übergeordnete Aspekte
DER.3.1 Audits und Revisionen	Informationsverbund/übergeordnete Aspekte
DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision	nicht relevant
DER.4 Notfallmanagement	Informationsverbund/übergeordnete Aspekte
APP.1.1 Office-Produkte	A10
APP.1.2 Webbrowser	A10
APP.1.4 Mobile Anwendungen (Apps)	S14, S15
APP.2.1 Allgemeiner Verzeichnisdienst	A15
APP.2.2 Active Directory Domain Services	A15
APP.2.3 OpenLDAP	A15
APP.3.1 Webanwendungen und Webservices	A09
APP.3.2 Webserver	S11
APP.3.3 Fileserver	A17

Baustein	Zielobjekte
APP.3.4 Samba	nicht relevant
APP.3.6 DNS-Server	A15
APP.4.2 SAP-ERP-System	nicht relevant
APP.4.3 Relationale Datenbanken	S04, S08
APP.4.4 Kubernetes	nicht relevant
APP.4.6 SAP ABAP-Programmierung	nicht relevant
APP.5.2 Microsoft Exchange und Outlook	A10
APP.5.3 Allgemeiner E-Mail-Client und -Server	A10
APP.5.4 Unified Communications und Collaboration (UCC)	A07, A08, S09, S10, NET
APP.6 Allgemeine Software	A01, A02, A03, A04, A05, A06, A07, A08, A09, A10, A11, A12, A13, A14, A15, A16, A17, A18
APP.7 Entwicklung von Individualsoftware	nicht relevant
SYS.1.1 Allgemeiner Server	S01, S02, S03, S04, S05, S07, S08, S09, S10, S11, S18, S19, S20, S21
SYS.1.2.2 Windows Server 2012	S01, S03, S04, S05, S07, S08, S09, S10, S11, S18, S19, S21
SYS.1.2.3 Windows Server	S01, S03, S04, S05, S07, S08, S09, S10, S11, S18, S19, S21
SYS.1.3 Server unter Linux und Unix	S01, S03, S04, S05, S07, S08, S09, S10, S11, S18, S19, S21
SYS.1.5 Virtualisierung	S21
SYS.1.6 Containerisierung	nicht relevant
SYS.1.7 IBM Z	nicht relevant
SYS.1.8 Speicherlösungen	S20
SYS.1.9 Terminalserver	nicht relevant
SYS.2.1 Allgemeiner Client	C01, C02
SYS.2.2.3 Clients unter Windows	C01, C02
SYS.2.3 Clients unter Linux und Unix	nicht relevant
SYS.2.4 Clients unter macOS	nicht relevant
SYS.2.5 Client-Virtualisierung	nicht relevant
SYS.2.6 Virtual Desktop Infrastructure	nicht relevant
SYS.3.1 Laptops	C01, C02
SYS.3.2.1 Allgemeine Smartphones und Tablets	S14, S15
SYS.3.2.2 Mobile Device Management (MDM)	Informationsverbund/übergeordnete Aspekte
SYS.3.2.3 iOS (for Enterprise)	S14, S15

Baustein	Zielobjekte
SYS.3.2.4 Android	S14, S15
SYS.3.3 Mobiltelefon	S14, S15
SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte	S13, S17, S22
SYS.4.3 Eingebettete Systeme	nicht relevant
SYS.4.4 Allgemeines IoT-Gerät	nicht relevant
SYS.4.5 Wechseldatenträger	Informationsverbund/übergeordnete Aspekte
NET.1.1 Netzarchitektur und -design	NET
NET.1.2 Netzmanagement	NET
NET.2.1 WLAN-Betrieb	NET
NET.2.2 WLAN-Nutzung	NET
NET.3.1 Router und Switches	NET
NET.3.2 Firewall	NET
NET.3.3 VPN	NET
NET.3.4 Network Access Control	nicht relevant
NET.4.1 TK-Anlagen	S16
NET.4.2 VoIP	A11
NET.4.3 Faxgeräte und Faxserver	S02
IND.1 Prozessleit- und Automatisierungstechnik	nicht relevant
IND.2.1 Allgemeine ICS-Komponente	nicht relevant
IND.2.2 Speicherprogrammierbare Steuerung (SPS)	nicht relevant
IND.2.3 Sensoren und Aktoren	nicht relevant
IND.2.4 Maschine	nicht relevant
IND.2.7 Safety Instrumented Systems	nicht relevant
IND.3.2 Fernwartung im industriellen Umfeld	nicht relevant
INF.1 Allgemeines Gebäude	G1
INF.2 Rechenzentrum sowie Serverraum	R1
INF.5 Raum sowie Schrank für technische Infrastruktur	R2
INF.6 Datenträgerarchiv	nicht relevant
INF.7 Büroarbeitsplatz	R4
INF.8 Häuslicher Arbeitsplatz	R5
INF.9 Mobiler Arbeitsplatz	R5
INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume	R7

Baustein	Zielobjekte
INF.11 Allgemeines Fahrzeug	nicht relevant
INF.12 Verkabelung	G1
INF.13 Technisches Gebäudemanagement	nicht relevant
INF.14 Gebäudeautomatisierung	nicht relevant

*Tabelle 13: Modellierung der Bausteine*

Für die nachfolgenden Zielobjekte ist zu prüfen, ob diese im jeweiligen konkreten Anwendungsszenario mit den existierenden Bausteinen des IT-Grundschutz-Kompendiums hinreichend abgebildet (modelliert) werden können:

- A01
- A03
- A04
- A05
- A06
- A12
- A13
- A14
- A16
- S22
- R3
- R7

## 10.2 Relevanz der Anforderungen

Nachdem die relevanten Bausteine des IT-Grundschutz-Kompendiums identifiziert worden sind, wird bei der Erstellung von IT-Grundschutzprofilen im nächsten Schritt eine zielgruppengerechte Anpassung der Anforderungen vorgenommen. In den Bausteinen werden Anforderungen vorgeschlagen, die typischerweise für diese Komponenten geeignet und angemessen sind. Für die Erstellung eines IT-Grundschutzprofils müssen die einzelnen Anforderungen durchgearbeitet werden und, wenn nötig, an die Rahmenbedingungen des IT-Grundschutz- Profils angepasst werden.

Es kann beispielsweise sinnvoll sein:

- alle Anforderungen eines Bausteins als relevant zu identifizieren,
- nur bestimmte Anforderungen als relevant zu identifizieren (z. B. nur Basis-Anforderungen),



- Anforderungen zu konkretisieren, also zum Beispiel, um weitere Aspekte zu ergänzen, oder
- Anforderungen komplett zu streichen.

Nicht nur vorhandene Anforderungen aus den IT-Grundschutz-Bausteinen können dem IT-Grundschutzprofil zugeordnet werden. In der Praxis wird es häufig erforderlich sein, zusätzliche Anforderungen zu identifizieren die für den betrachteten Informationsverbund von Bedeutung sind. Dies ist beispielsweise dann der Fall, wenn erhöhter Schutzbedarf vorliegt. Auch wenn einzelne Zielobjekte der Referenzarchitektur nicht oder nicht hinreichend mit bestehenden Bausteinen aus dem IT-Grundschutz-Kompendium abgebildet werden können, müssen weitere Anforderungen ergänzt werden.

Auf diese Weise kann mit Hilfe der IT-Grundschutzprofile ein Sicherheitsniveau erreicht werden, das exakt dem Schutzbedarf des betrachteten Anwendungsbereiches entspricht.

## 11 Restrisiko

Bei der Erstellung von IT-Grundschutzprofilen werden im Rahmen von Risikoanalysen in der Regel ergänzende Sicherheitsanforderungen identifiziert, die über das IT-Grundschutz-Modell hinausgehen. Dabei werden typischerweise auch Risiken gefunden, die nicht alle durch vorgegebene Anforderungen bzw. dazugehörige Maßnahmen abgedeckt werden können. Solche Restrisiken müssen bewertet und dokumentiert werden. So sollte unter anderem aufgenommen werden, wenn vorhandene (Standard-)Anforderungen eines Bausteins nicht erfüllt werden oder wenn mit zusätzlichen Maßnahmen mehr Risiken abgedeckt werden könnten.

Darüber hinaus können sich im Einzelfall zusätzliche Risiken ergeben, die im Rahmen des Informationssicherheitsmanagements behandelt werden müssen.

## 12 Unterstützende Informationen

Dokument	Ansprechpartner
Datenschutzkonzept für die elektronische Aktenbearbeitung mit der Software VIS-Justiz	Bundespatentgericht Bundesgerichtshof
Sicherheitskonzept für das Fachsystem Goša	Anwenderkreis Goša Bundesverwaltungsgericht
IT-Grundschutzprofil Bundesgerichte.vna (Edition 2023)	Anlage zum Dokument