



Sachsen-Anhalt | IT-Grundschutz-Profil

Einnahmeverwaltung des Ministeriums der Finanzen Sachsen-Anhalt

Dokumenteneigentümer	Ministerium der Finanzen Sachsen-Anhalt
Version	1.0
Stand	07.09.2023
Revisionszyklus	2 Jahre
Status	gültig
Vertraulichkeitsstufe:	TLP: White

Formale Aspekte

Titel	IT-Grundschutz-Profil der Einnahmeverwaltung des Ministeriums der Finanzen Sachsen-Anhalt [IT-Grundschutz-Profil Finanzamt]
Autoren	Ortholf, Christian Frenzel, Philipp Juhnke, Dirk Suchold, Nico
Herausgeber	Informationssicherheitsbeauftragte/r Ministerium für Finanzen Sachsen-Anhalt Editharing 40 30108 Magdeburg
Versionsstand	1.0
Stand	07.09.2023
Revisionszyklus	2 Jahre
Vertraulichkeit	TLP: White

Änderungshistorie

Ver- sion	Stand	Bearbeiter	Änderungen / Kommentar
0.8	22.11.2022	Frenzel, Philipp Ortholf, Christian Juhnke, Dirk	Initiale Erstellung, Arbeitsversion für BSI
0.9	20.03.2023	Frenzel, Philipp	Qualitätssicherung, Anpassungen des BSI
1.0	07.09.2023	Frenzel, Philipp Ortholf, Christian Juhnke, Dirk Suchold, Nico	Freigabe durch Amtschef Ministerium der Finanzen Sachsen-Anhalt

Inhaltsverzeichnis

Management Summary	7
1 Formalitäten	8
1.1 Zielsetzung.....	8
1.2 Struktur des IT-Grundschatz-Profiles	8
1.3 Vorgaben zum ISMS	8
1.4 Anwendung	9
1.5 Verantwortlichkeiten und Verpflichtung	9
1.6 Geltungsdauer	9
1.7 Revision	9
1.8 Begrifflichkeiten.....	9
1.9 Verbindlichkeit von Formulierungen	10
2 Festlegung des Geltungsbereichs.....	12
2.1 Geltungsbereich und Abgrenzung	12
2.2 Anwendungsbereich.....	12
2.3 Organisatorische Struktur.....	13
2.4 Schutzbedarf.....	13
2.5 IT-Grundschatz-Vorgehensweise	13
2.6 Rahmenbedingungen.....	14
3 Strukturanalyse – Definition des Informationsverbunds	15
3.1 Allgemeines	15
3.2 Angrenzende Informationsverbünde und Organisationen.....	15
3.3 Geschäftsprozesse	17
3.3.1 Leistungsprozesse.....	18
3.3.2 Unterstützungsprozesse	18
3.4 Referenzarchitektur.....	19
3.5 Netzplan.....	20
4 Schutzbedarfsfeststellung	22
5 Modellierung	23
6 Zu erfüllende Anforderungen und umzusetzende Maßnahmen.....	24
6.1 Ausgeschlossene und an anderen Stellen bearbeitete Anforderungen aus Bausteinen.....	24
6.2 Ausgeschlossene oder an anderer Stelle bearbeitete Anforderungen aus IT-Systemen.....	25
6.2.1 Zielobjekt IT03.....	25
6.2.2 Zielobjekt IT04.....	25

6.2.3	Zielobjekt IT05	25
6.2.4	Zielobjekt IT07	26
6.2.5	Zielobjekt IT08, IT09, IT10 und IT11	26
7	Risikoanalyse	28
8	Anwendungshinweise	29
8.1	Allgemeines	29
8.2	Implementierung	29
8.3	Weiterentwicklung	30
9	Abkürzungen.....	31
10	Referenzen	32
11	Anlagen	33

Tabellenverzeichnis

Tabelle 1: Struktur des IT-Grundschutz-Profils	8
Tabelle 2: Begrifflichkeiten	10
Tabelle 3: Verbindlichkeit von Festlegungen	11
Tabelle 4: Finanzämter in Sachsen-Anhalt	13
Tabelle 5: Zuständigkeiten und Verantwortlichkeiten im Kontext der Einnahmeverwaltung ..	16
Tabelle 6: Zielobjekte	20
Tabelle 7: Anforderungen des Zielobjekts IT03	25
Tabelle 8: Anforderungen des Zielobjekts IT04	25
Tabelle 9: Anforderungen des Zielobjekts IT05	26
Tabelle 10: Anforderungen des Zielobjekts IT07	26
Tabelle 11: Anforderungen der Zielobjekte IT08, IT09, IT10 und IT11	27
Tabelle 12: Abkürzungen	31
Tabelle 13: Referenzen	32
Tabelle 14: Anlagen	33

Abbildungsverzeichnis

Abbildung 1: Übersicht Absicherungen	14
Abbildung 2: Vorgehen Standard-Absicherung	14
Abbildung 3: Abgrenzung der Dienstleister	16
Abbildung 4: Abgrenzung der Informationsverbünde	17
Abbildung 5: Prozesslandkarte	18
Abbildung 6: Abgrenzung der Anwendungen	20
Abbildung 7: Netzplan	21
Abbildung 8: Zeitliche Umsetzung des IT-Grundschutz-Profils	29

Management Summary

Das vorliegende IT-Grundschutz-Profil wurde für die Finanzämter des Landes Sachsen-Anhalt entwickelt. Es dient als Mustervorlage für den einheitlichen Aufbau und Betrieb eines Managementsystems für Informationssicherheit in der Einnahmeverwaltung Sachsen-Anhalt.

Mit dem Ziel einer Standard-Absicherung auf Basis des IT-Grundschutzes mit einem hohen Schutzbedarf werden die folgenden Geschäftsprozesse eines Finanzamtes betrachtet:

1) Leistungsprozesse:

- Innendienst steuerliche Verfahren
- Außendienst steuerliche Verfahren

2) Unterstützungsprozesse:

- Personal
- Organisation
- Informations- und Kommunikationstechnik
- Finanzen

Hierzu werden zunächst die Zielobjekte, die Referenzarchitektur und die jeweiligen Schutzbedarfe beschrieben. Ein besonderes Augenmerk liegt auf den eingesetzten Dienstleistern. Im Rahmen der Modellierung werden die für die Zielobjekte erforderlichen IT-Grundschutz-Bausteine identifiziert. Da für das Steuerfachverfahren und den eingesetzten Steuerclient ein hoher Schutzbedarf festgestellt wurde, ist nach der IT-Grundschutz-Methodik eine Risikoanalyse für die entsprechenden Zielobjekte durchzuführen. Im Ergebnis wird so festgestellt, welche zusätzlichen Maßnahmen noch umgesetzt werden können, um dem hohen Schutzbedarf Genüge zu tun.

Das IT-Grundschutz-Profil wird in jedem Finanzamt einheitlich angewandt. Es kann bei festgestelltem Bedarf auch spezifisch angepasst und/oder ergänzt werden, um konkrete örtliche oder organisationsbedingte Besonderheiten angemessen zu berücksichtigen.

Die IT-Netzwerkinfrastruktur und die IT-Fachverfahren in den jeweiligen Finanzämtern werden von unterschiedlichen IT-Dienstleistern im Auftrag des Landes betrieben. Für die bauliche Infrastruktur der Finanzämter ist der Landesbetrieb Bau- und Liegenschaftsmanagement Sachsen-Anhalt (BLSA) zuständig und am Markt tätige Unternehmen bei Mietobjekten.

Das vorliegende IT-Grundschutz-Profil berücksichtigt die Zusammenarbeit mit den Dienstleistern, nimmt erforderliche Abgrenzungen hinsichtlich der Zuständigkeiten bzw. Verantwortungsbereiche vor und beschreibt die entsprechenden Schnittstellen hierfür. Die im IT-Grundschutz-Profil enthaltenen Anforderungen aus dem IT-Grundschutz-Kompendium müssen auch an diese Dienstleister gestellt werden und sollten daher in den entsprechenden vertraglichen Regelungen Berücksichtigung finden.

1 Formalitäten

1.1 Zielsetzung

Das vorliegende Dokument stellt ein IT-Grundschutz-Profil nach den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) dar. Es wurde mit folgender Zielstellung entwickelt:

- ein idealtypisches Finanzamt im Bundesland Sachsen-Anhalt abzubilden,
- alle relevanten IKT-Systeme zu erfassen und die Rollen, sowie Zuständigkeiten darzustellen,
- die Grundlage für einen BSI-konformen und dem Stand der Technik entsprechenden Betrieb zu schaffen.

Das Risiko der Verletzung der Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität wird dadurch minimiert.

1.2 Struktur des IT-Grundschutz-Profiles

Das IT-Grundschutz-Profil folgt der Struktur, basierend auf [Ref. 04]:

Bezeichnung	Inhalt	Kapitel
A.1	Strukturanalyse	3
A.2	Schutzbedarfsfeststellung	4
A.3	Modellierung	5
A.4	IT-Grundschutz-Check	6
A.5	Risikoanalyse	7
A.6	Realisierungsplan	8

Tabelle 1: Struktur des IT-Grundschutz-Profiles

In den jeweiligen Kapiteln werden die allgemein gültigen Vorgaben, minimal geltenden Randbedingungen und Anforderungen definiert. Die Nachweisdokumente (A.1 bis A.6) sind gemäß [Ref.04] aufgebaut.

1.3 Vorgaben zum ISMS

Ein Informationssicherheitsmanagementsystem (ISMS) ist ein Managementsystem, welches zum Ziel hat, Informationen jeglicher Art, die in Geschäftsprozessen generiert, genutzt oder verarbeitet werden zu schützen. Hierbei ist unabhängig, ob die Informationen analog oder digital vorliegen bzw. verarbeitet werden. Die Informationssicherheit hat das Ziel, die Informationen nach den Grundwerten Verfügbarkeit, Vertraulichkeit und Integrität zu schützen. Aufbauend auf den aktualisierten Beschluss des IT-Planungsrates aus dem Jahr 2019 und dem damit direkt in Zusammenhang stehenden Umsetzungsplan aus 2022¹ ist in den Bundesländern ein Mindestniveau an Informationssicherheit zu erreichen.

Das ISMS im Geschäftsbereich ist gemäß Ziffer 4 der LL IS [vgl. Ref. 01] auf der Grundlage des IT-Grundschatzes des BSI (Bundesamt für Sicherheit in der Informationstechnik) basierend auf der ISO

¹ <https://www.it-planungsrat.de/projekte/umsetzung-der-leitlinie-fuer-informationssicherheit> [Stand: 20.03.2023]

27001 umzusetzen; hierfür werden die aktuell gültigen Standards des BSI herangezogen. Die Einnahmeverwaltung zählt zum Geschäftsbereich des Ministeriums (MF ST) der Finanzen.

Die seitens der/des Informationssicherheitsbeauftragten (ISB) definierten und seitens der Amtsleitung verabschiedeten Methoden, Vorgaben und Empfehlungen für Organisation, Prozesse und IT-Systeme sind verbindlich umzusetzen und gelten uneingeschränkt mit.

1.4 Anwendung

Die Anwendung dieses IT-Grundschutz-Profiles gilt für die Einnahmeverwaltung ST und alle Mitarbeitenden. Verantwortlich für die Umsetzung sind die Amtsleitung und die Sachgebietsleitung im Rahmen des Zuständigkeitsbereichs. Das IT-Grundschutz-Profil gilt für Geschäftsprozesse, Gebäude, Räume, IT-Systeme und Fachverfahren und ist adaptiert zur Anwendung zu bringen.

Die identifizierten Anforderungen werden entweder als (vertragliche) Anforderungen an die jeweiligen Dienstleister gestellt oder für die in eigener Verantwortung stehenden Infrastrukturen und ITK-Systeme über den IT-Grundschutz-Check (GSC) beantwortet.

Die sich aus dem Vertragsverhältnissen zu den jeweiligen Dienstleistern ergebenden Risiken können aufgenommen und behandelt werden.

Eine detaillierte Vorgehensweise zur Anwendung findet sich in Kap. 8.

1.5 Verantwortlichkeiten und Verpflichtung

Das IT-Grundschutz-Profil richtet sich an die Einnahmeverwaltung ST und damit an alle Finanzämter (FA) im Bundesland. Dies schließt das Personal, den zuständigen Bereichs-ISB im Finanzamt am Standort, den ISB des Ministeriums der Finanzen und die Aufbauorganisation mit ein, wenngleich diese nur als Schnittstelle betrachtet werden.

Für die Betreuung des IT-Grundschutz-Profiles ist der ISB MF ST zuständig. Dieser überwacht die Initiierung und Umsetzung von Maßnahmen resultierend aus der Anwendung des IT-Grundschutz-Profiles für das Finanzamt. Die Bereichs-ISB im Finanzamt sind im Rahmen ihrer Zuständigkeit für die Gewährleistung der Informationssicherheit verantwortlich.

Die Verantwortung für die Umsetzung dieses IT-Grundschutz-Profiles trägt die Amtsleitung. Die Umsetzung ist verpflichtend und wird durch den ISB MF ST initiiert und kontrolliert.

1.6 Geltungsdauer

Das vorliegende Dokument tritt am Tag nach der Veröffentlichung in Kraft und gilt bis zum Erscheinen einer neuen Version bzw. bis auf Widerruf.

1.7 Revision

Das IT-Grundschutz-Profil wird vom ISB MF ST in zweijährlichen Abständen oder anlassbezogen auf Aktualität und Vollständigkeit hin überprüft und bei Bedarf angepasst.

1.8 Begrifflichkeiten

Die in den folgenden Kapiteln benutzten Begriffe entsprechen folgenden Bedeutungen:

Begriff	Bedeutung
Amtsleitung	Die Amtsleitung im Kontext dieses IT-Grundschutz-Profiles umfasst die/ den Amtsleiter/in und ihre/ seinen Stellvertreter/in.
Einnahmeverwaltung	Die Einnahmeverwaltung nimmt sämtliche Steuern ein, die durch die Landesgesetzgebung festgesetzt und erhoben werden dürfen und können. Gleichzeitig werden Steuern auf Grundlage der Bundesgesetzgebung eingenommen; kommunale Steuern kann dies, im Rahmen der hoheitlichen Aufgabenübertragung, ebenso betreffen.
Finanzamt	Ein Finanzamt ist eine örtliche Landesbehörde zum Vollziehen der geltenden Steuergesetzgebung. Ein Finanzamt ist ein Teil der Einnahmeverwaltung.
Informationsverbund	Der Informationsverbund stellt den zu betrachtenden Teil des Geltungsbereichs, für die Anwendung der Sicherheitsbetrachtung dar.
IT-Grundschutz-Check (GSC)	Der IT-Grundschutz-Check stellt einen Soll-Ist-Vergleich der Anforderungen der Bausteine aus dem BSI-Grundschutz-Kompendium dar und zeigt die umzusetzenden Maßnahmen auf.
Referenzarchitektur	Die Referenzarchitektur gibt eine Übersicht über alle Zielobjekte. Dazu zählen alle physischen, virtuellen und organisatorischen Systeme. Die Referenzarchitektur dient mit ihrem Inhalt als Grundlage für die Modellierung.
Risikoanalyse	Die Risikoanalyse ist ein systematischer Prozess zur Identifikation, Einschätzung und Bewertung von Risiken, die unterschiedliche Ursachen haben können. Für die identifizierten elementaren Gefährdungen und Anforderungen, die durch die entwickelten Maßnahmen auf Grundlage eines IT-Grundschutz-Check nicht abgedeckt werden können, ist eine Risikoanalyse erforderlich; ebenso, wenn der ermittelte Schutzbedarf über „normal“ liegt.

Tabelle 2: Begrifflichkeiten

Weitere Rollen sind in der Organisationsrichtlinie (vgl. [Ref. 03]) beschrieben und werden dort mit Aufgaben und Zuständigkeit beschrieben.

1.9 Verbindlichkeit von Formulierungen

Es werden Modalverben in diesem IT-Grundschutz-Profil genutzt. Die nachfolgenden Begriffe basieren auf den Definitionen des BSI und werden entsprechend ihrer Bedeutung in diesem Dokument benutzt.

Begriff	Bedeutung
MUSS, DARF NUR	Dieser Ausdruck bedeutet, dass es sich um eine Anforderung handelt, die unbedingt erfüllt werden muss (uneingeschränkte Anforderung).
DARF NICHT, DARF KEIN	Dieser Ausdruck bedeutet, dass etwas in keinem Fall getan werden darf (uneingeschränktes Verbot).

Begriff	Bedeutung
SOLLTE	Dieser Ausdruck bedeutet, dass eine Anforderung normalerweise erfüllt werden muss, es aber Gründe geben kann, dies doch nicht zu tun. Dies muss aber sorgfältig abgewogen und stichhaltig begründet werden.
SOLLTE NICHT, SOLLTE KEIN	Dieser Ausdruck bedeutet, dass etwas normalerweise nicht getan werden sollte, es aber Gründe gibt, dies doch zu tun. Dies muss aber sorgfältig abgewogen und stichhaltig begründet werden.

Tabelle 3: Verbindlichkeit von Festlegungen

2 Festlegung des Geltungsbereichs

Der Informationsverbund definiert den Geltungsbereich des Sicherheitskonzepts.

2.1 Geltungsbereich und Abgrenzung

Der Geltungsbereich umfasst das jeweilige Finanzamt (FA). Darin ist enthalten:

- die Geschäftsprozesse der Einnahmeverwaltung,
- die Anwendungen und IT-Systeme, die zur Durchführung oder Unterstützung der Geschäftsprozesse notwendig sind,
- alle Infrastrukturen (z. B. Gebäude, Räume), die für die Aufgabenerfüllung und für die Geschäftsprozesse benötigt werden,
- die telekommunikationstechnische Ausstattung für die Aufgabenerfüllung (z. B. Faxgeräte, Drahtlostelefone) und
- die Sicherheitstechnik (z. B. Schließ- und Einbruchmeldeanlage).

Nicht zum Informationsverbund gehören:

- das Steuerfachverfahren und weitere genutzte Anwendungen, Applikationen und Systeme (z. B. Steuerclient, Standard-Arbeitsplatz), die nicht durch das FA selbst, sondern durch einen oder mehrere Dienstleister betrieben werden,
- die Netzwerktechnik und Netze, die separiert sind (z. B. Landesdatennetz),
- Multimedialechnik (z. B. TV-Geräte, Beamer), die nicht mit einem Netzwerk verbunden sind.

Die nicht zum hier betrachteten Informationsverbund gehörenden Systeme werden durch Dienstleister (Outsourcing) bereitgestellt und im Auftrag des Ministeriums der Finanzen bereitgestellt. Die Aufteilung und Abgrenzung sind in Tabelle 5 zu finden.

Jedes FA ist als ein eigenständiger Informationsverbund definiert. Dieser muss das gesamte FA umfassen. Ein FA darf nicht mehrere Informationsverbünde pflegen.

2.2 Anwendungsbereich

Das IT-Grundschatz-Profil wird auf folgende FA angewendet:

Standort	Finanzamtsnummer
Bitterfeld-Wolfen	3116
Dessau-Roßlau	3114
Lutherstadt Eisleben	3118
Genthin	3103
Haldensleben	3105
Halle (Saale)	3110
Magdeburg	3102
Merseburg	3112
Naumburg	3119
Quedlinburg	3117
Salzwedel	3106

Standort	Finanzamtsnummer
Staßfurt	3107
Stendal	3108
Lutherstadt Wittenberg	3115

Tabelle 4: Finanzämter in Sachsen-Anhalt

Das FA Dessau-Roßlau (3114) nimmt eine Sonderaufgabe wahr. Es existiert eine Außenstelle in Magdeburg mit besonderen Aufgaben im Bereich der Finanzdienstleistungen.

Weitere lokationsspezifische Besonderheiten sind im Rahmen der Anwendung des IT-Grundschutz-Profils zu berücksichtigen und kenntlich zu machen.

2.3 Organisatorische Struktur

Organisatorisch gliedert sich ein FA in Sachgebiete, welche wiederum mehrere Arbeitsgebiete umfassen können. Das Arbeitsgebiet ist die kleinste Organisationseinheit, dem bestimmte, abgegrenzte Aufgaben zugewiesen sind. Die Amtsleitung leitet das FA und wird von der obersten Landesfinanzbehörde bestellt. Sie ist Vorgesetzte aller Beschäftigten und Dienstvorgesetzte der Beamtenschaft. Die Amtsleitung trägt die Verantwortung für die rechtzeitige, sachgerechte und wirtschaftliche Erfüllung der Aufgaben des Finanzamts (Fach- und Dienstaufsicht). Dies umfasst auch die Bereiche Informationssicherheit und Datenschutz. Hierzu nutzt die Amtsleitung die vorhandenen Steuerungs- und Führungsinstrumente.

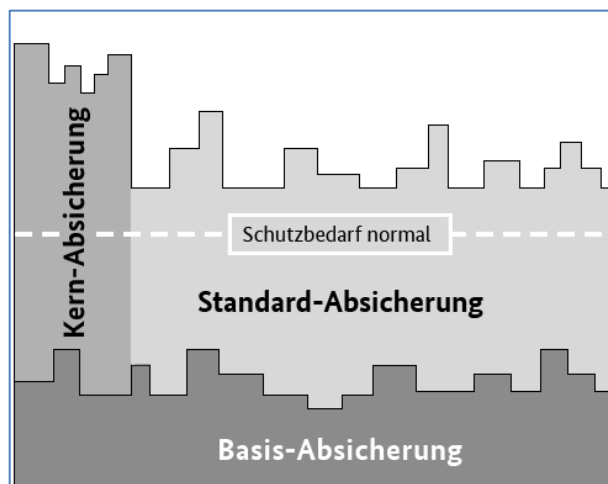
Soweit sichergestellt ist, dass die durch dieses IT-Grundschutz-Profil festgelegten Mindestanforderungen vollständig umgesetzt werden, ist die weitere Ausgestaltung der Maßnahmen in Art und Umfang freigestellt.

2.4 Schutzbedarf

Das vorliegende IT-Grundschutz-Profil beschreibt ein Schutzniveau mit **hohem Schutzbedarf**. Das resultiert aus der Schutzbedarfsfeststellung (vgl. Kap. 4), die auf Vererbungseffekten basiert.

2.5 IT-Grundschutz-Vorgehensweise

Die Vorgehensweise richtet sich nach der Standard-Absicherung gemäß BSI-Standard 200-2 [Ref. 06].



Die nachfolgende Abbildung stellt den Ablauf der Standard-Absicherung dar.

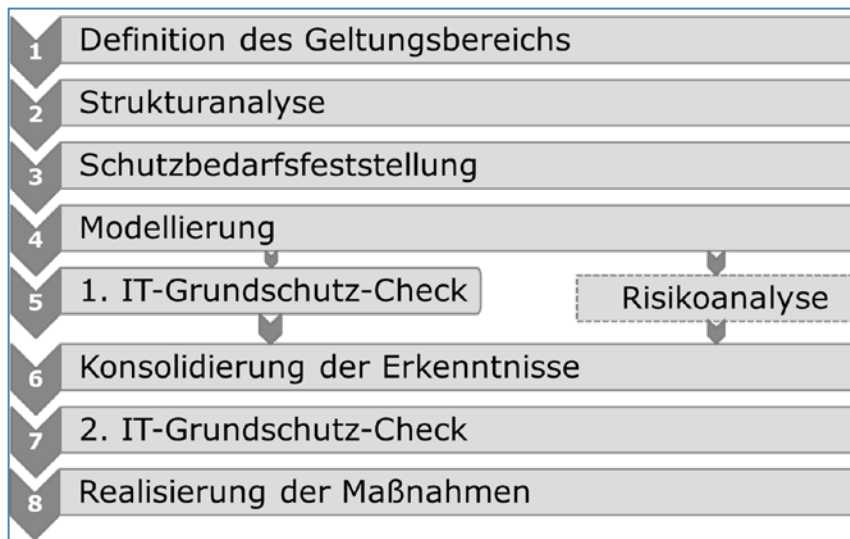


Abbildung 2: Vorgehen Standard-Absicherung

Das Vorgehen gemäß Standard-Absicherung ist individuell für jedes Finanzamt durchzuführen. Es obliegt den Aufgaben des Bereichs-ISB, die nicht abgegrenzten Fachverfahren und IT-Infrastrukturen durch weitere Maßnahmen, auf Grundlage des konkret definierten Schutzbedarfs, zu schützen.

Das Finanzamt führt individuell und IT-gestützt die Nachweise der IT-Grundschutz-Checks und der Risikoanalysen durch. Dieses IT-Grundschutz-Profil liefert eine Anleitung hierfür. Es werden standardisierte Vorlagen genutzt, die durch den ISB des MF ST vorgegeben werden. Es handelt sich um Vorgaben und Vorlagen gemäß der Struktur des IT-Grundschutzprofils (vgl. Kap. 1.2).

Für die erstmalige Anwendung des IT-Grundschutz-Profiles kann die Basis-Absicherung erstmalig implementiert werden (vgl. Kap. 8.2).

2.6 Rahmenbedingungen

Das vorliegende Dokument betrachtet das Objekt „Finanzamt“ (FA) auf einer allgemeinen Basis. Dabei werden Standortspezifika im Rahmen dieses allgemein anwendbaren IT-Grundschutz-Profiles, z. B. Lage oder konkret hochbauliche Bewertungen, nicht betrachtet.

Es werden grundsätzlich identische Anforderungen gestellt, welche betrachtet und bewertet werden. Zur Ermittlung der erforderlichen Anforderungen wird das BSI-Grundschutz-Kompodium 2022 (Stand Februar 2022) herangezogen. Die Aktualisierung erfolgt im Rahmen der zweijährlichen Revisionierung.

3 Strukturanalyse – Definition des Informationsverbunds

Die Anwendung des IT-Grundschutz-Profiles erfolgt in der Hoheit des spezifischen FA. Der Informationsverbund repräsentiert in der Anwendung des IT-Grundschutz-Profiles das konkrete FA. Die Abgrenzung ist in Abbildung 4 ersichtlich. Die Strukturanalyse, als Grundlage für den Informationsverbund, ist in A.1 zu finden.

3.1 Allgemeines

Der zu schützende Informationsverbund bestimmt sich aus den zu erfüllenden Fachaufgaben. Die Aufgaben werden in § 17 Finanzverwaltungsgesetz – FVG bestimmt und konkretisieren sich wie folgt:

- die Festsetzung und Erhebung von Steuern und Nebenleistungen,
- die Übermittlung der Steuererklärung an das Finanzamt,
- die Erstellung einer Einspruchsentscheidung und
- die Durchführung einer Betriebsprüfung.

Aufbauend auf den Fachaufgaben werden Geschäftsprozesse zur Erfüllung dieser definiert. Zur Umsetzung der Geschäftsprozesse können Anwendungen, IT-Systeme, Netze und Komponenten, Gebäude und Räume genutzt werden.

Aufgrund der zentralisierten Dienstleisterstruktur im Land Sachsen-Anhalt ist eine Abgrenzung der Verantwortungs- und Zuständigkeitsbereiche erforderlich.

3.2 Angrenzende Informationsverbünde und Organisationen

Die Einnahmeverwaltung wird durch unterschiedliche landeseigene und externe Dienstleister (Organisationen) betreut. Für diese sind eigene Informationsverbünde definiert bzw. fordernd zu definieren. Gleichzeitig existieren übergeordnete Organisationsstrukturen, die überwachend, regelnd und richtlinienkompetent auf die Einnahmeverwaltung einwirken. Diese werden grundsätzlich in der Strukturanalyse betrachtet, aber im Rahmen der Modellierung, Schutzbedarfsfeststellung und Risikoanalyse nicht gesondert betrachtet.

Die Unterscheidung und Zusammenhänge der Informationsverbünde und Organisationen sind nachfolgend dargestellt. Zu beachten ist hierbei, dass für die Einnahmeverwaltung eine Verpflichtung besteht, ausgewählte Dienstleister zu nutzen, die durch eine zentrale Stelle beauftragt werden. Gleichzeitig werden organisatorische Abläufe und Aufbauorganisationen im Rahmen von übergreifenden Regelungen genutzt. Dies trifft im Wesentlichen auf das Notfallmanagement zu.

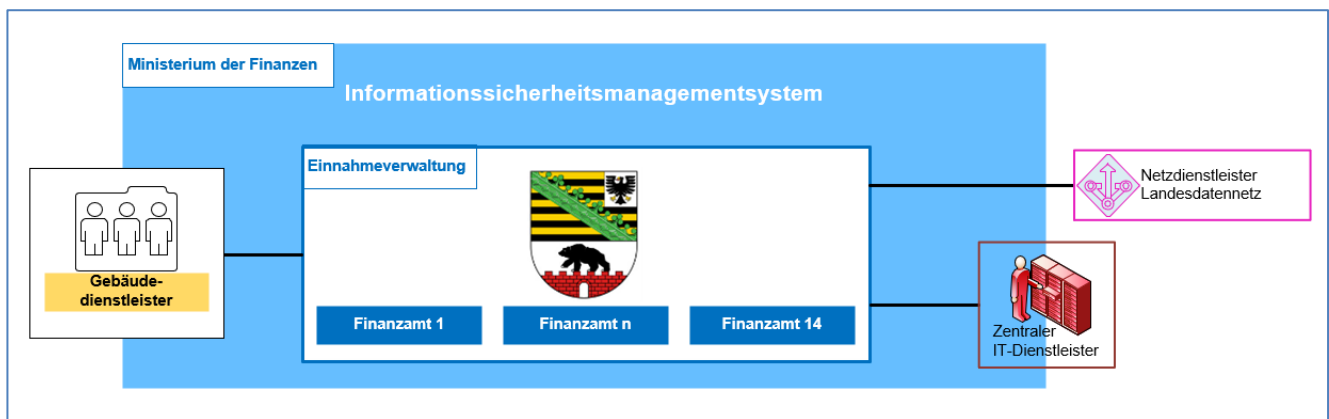


Abbildung 3: Abgrenzung der Dienstleister

Hieraus abgeleitet ergibt folgende Zuständigkeit, sodass die nachfolgende Tabelle 5 einen Überblick der zum Einsatz kommenden zentralen Komponenten gibt:

Bezeichnung / Zuständigkeiten	Netzdienst- leister Lan- desdaten- netz	Gebäude- dienstleis- ter	Zentraler IT- Dienstleis- ter	Finanzamt
ITN-XT	X			
Verkabelung	X	X		X
Arbeitsplatz				X
Mobiler Arbeitsplatz				X
IT-gestützte Büro- und Fachanwen- dungen			X	
Steuerfachverfahren			X	
Steuerclient fest			X	
Steuerclient mobil			X	X
Telefonanlage			X	
Telefon			X	
Faxgerät			X	X
Multifunktionsgerät			X	
Mobiler Drucker			X	X
Lokaler Drucker			X	X
Gebäude		X		
Räume				X
Technische Gebäudeausstattung		X		
Sicherheitstechnik		X		X

Tabelle 5: Zuständigkeiten und Verantwortlichkeiten im Kontext der Einnahmeverwaltung

Die Zuständigkeit der Dienstleister ist gemäß nachfolgender Abbildung 4 abgegrenzt.

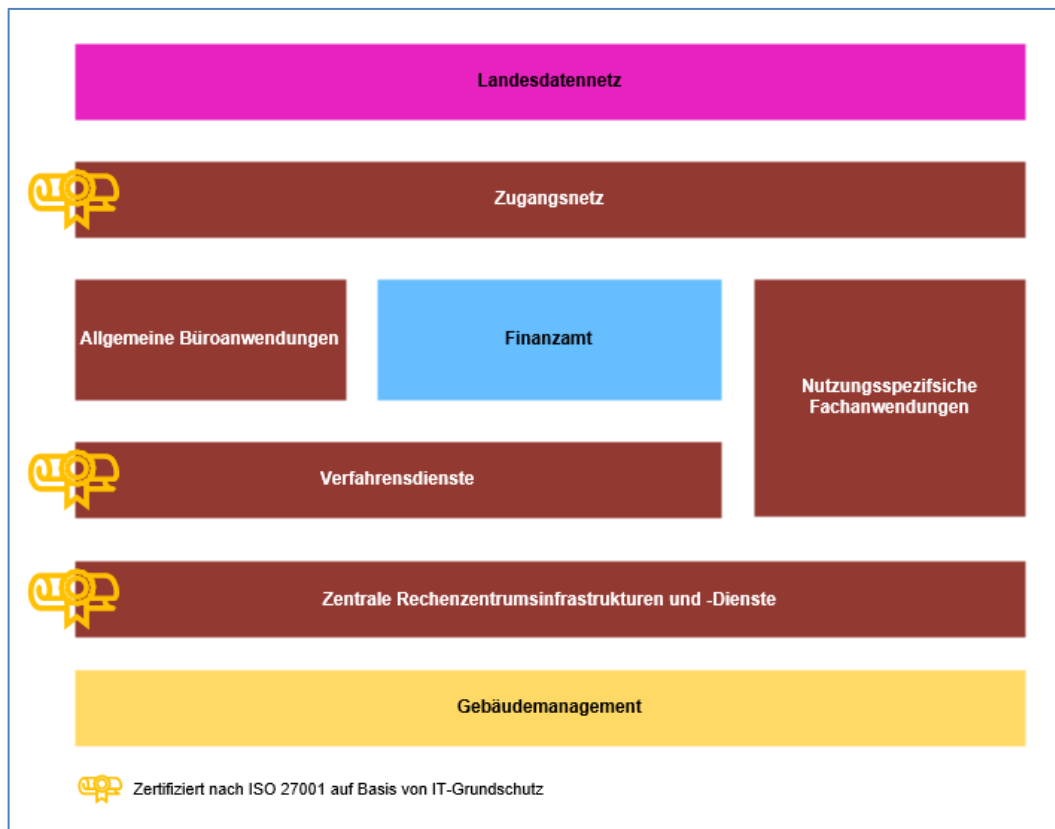


Abbildung 4: Abgrenzung der Informationsverbünde

Standortspezifische Besonderheiten, die sich nicht mit diesem IT-Grundschutz-Profil abbilden lassen, sind gesondert in der Anwendung des IT-Grundschutz-Profiles zu betrachten. Hierfür sind die Teile des Sicherheitskonzepts (vgl. Tabelle 1) an die realen Gegebenheiten anzupassen.

3.3 Geschäftsprozesse

Die Geschäftsprozesse leiten sich aus den Fachaufgaben (vgl. Kap. 3.1) ab. Sie müssen für die Betrachtung des Informationsverbunds übernommen werden.

Die Geschäftsprozesse unterscheiden sich in:

- **Steuerungsprozesse:**
Die Steuerungsprozesse repräsentieren die Fachaufsicht, welche durch das Ministerium der Finanzen erbracht wird. Als Besonderheit ist hier das Notfallmanagement zu erwähnen, welches im Ministerium und in der Einnahmeverwaltung gesteuert und ausgestaltet wird.
- **Leistungsprozesse:**
Die Leistungsprozesse definieren sich durch die konkrete Leistungserbringung des FA. Sie setzen die Fachaufgaben um.
- **Unterstützungsprozesse:**
Die Unterstützungsprozesse beschreiben die Grundlagen und Unterstützungsleistungen, welche zur Durchführung der Leistungsprozesse notwendig ist. Sie unterstützen die Leistungsprozesse mittelbar.

Zum Informationsverbund gehören die Leistungs- und Unterstützungsprozesse. Alle identifizierten Prozesse müssen einem Zielobjekt (Gebäude, IT-System, Anwendung) zugeordnet werden.

Die nachfolgende Prozesslandkarte stellt die Geschäftsprozesse des Informationsverbunds dar.

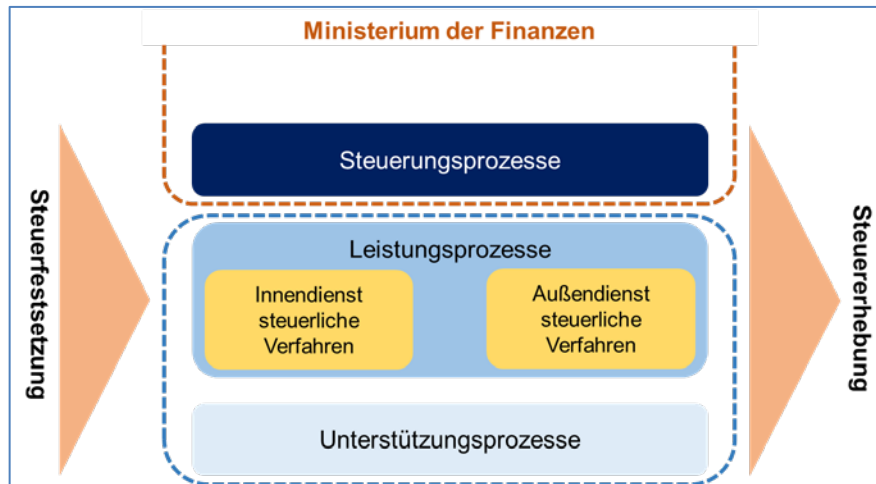


Abbildung 5: Prozesslandkarte

3.3.1 Leistungsprozesse

Zu den Leistungsprozessen zählen:

- Innendienst steuerliche Verfahren:
Der Leistungsprozess „Innendienst steuerliche Verfahren“ umfasst alle Tätigkeiten und Abläufe, die mit der Festsetzung und Erhebung von Steuern, den Prüfungsdiensten und sonstigen steuerlichen Fachaufgaben unmittelbar in Zusammenhang stehen und ganz oder zu großen Teilen am Innendienst arbeitsplatz eines FA wahrgenommen werden.
- Außendienst steuerliche Verfahren:
Der Leistungsprozess „Außendienst steuerliche Verfahren“ umfasst alle Tätigkeiten und Abläufe, die mit der Festsetzung und Erhebung von Steuern, den Prüfungsdiensten und sonstigen steuerlichen Fachaufgaben unmittelbar in Zusammenhang stehen und ganz oder zu großen Teilen im Außendienst eines FA wahrgenommen werden.

3.3.2 Unterstützungsprozesse

Zu den Unterstützungsprozessen gehören die nachfolgenden vier Prozesse:

Der Unterstützungsprozess „**Personal**“ umfasst die operative Ausgestaltung der zentralen Personalvorgaben seitens des Ministeriums der Finanzen. Der Prozess beinhaltet unterschiedliche Abläufe, Zuständigkeiten und Subprozesse. Hierbei handelt es sich um:

- Personalplanung und Personaleinsatzplanung
- Verwaltung von Personaldaten
- Besoldungsangelegenheiten
- Entgeltangelegenheiten
- Organisation und Abrechnung von Dienstreisen
- Verwaltung und Auswertung der Zeiterfassung (An- und Abwesenheiten)
- Aus- und Weiterbildung
- Ausbildungsleitung für Nachwuchskräfte

Der Unterstützungsprozess „**Organisation**“ beinhaltet Abläufe zur Aufrechterhaltung des Geschäftsbetriebs eines Finanzamts. Die Umsetzung folgt den Vorgaben des Ministeriums der Finanzen. Der

Prozess beinhaltet unterschiedliche Abläufe, Zuständigkeiten und Subprozesse. Hierbei handelt es sich um:

- Aufstellung und Pflege des Geschäftsverteilungsplans
- Inventarisierung
- Empfang und hausinterne Weiterleitung sowie Versand von Post- und Paketsendungen
- Scannen und Archivierung von Post- und Steuersachen
- Datenschutzkoordination
- Juristische Prüfungen und Stellungnahmen
- Führung des Archivs
- Verwaltung der Bücherei und Registratur
- Botendienste
- Hausmeisterangelegenheiten

Der Unterstützungsprozess „**Informations- und Kommunikationstechnik**“ (IKT) beinhaltet die operative Ausgestaltung der zentral verwalteten (Ministerium für Infrastruktur und Digitales, Ministerium der Finanzen) und erbrachten (Dienstleister) Leistungen. Der Prozess beinhaltet unterschiedliche Abläufe, Zuständigkeiten und Subprozesse. Hierbei handelt es sich um:

- Nutzung von aufgabenspezifischen Anwendungen
- Anforderungsmanagement für IKT an das MF
- Koordination der Nutzerbedarfe in Form von Störungsmeldungen
- Beschaffungsanforderungen von IKT an das MF

Der Unterstützungsprozess „**Finanzen**“ stellt sicher, dass die steuerlichen Resultate aus den Leistungsprozessen im Tätigkeitsbereich der Einnahmeverwaltung korrekt verbucht werden. Gleichzeitig werden damit die zentralen Vorgaben des Ministeriums der Finanzen umgesetzt. Der Prozess beinhaltet unterschiedliche Abläufe, Zuständigkeiten und Subprozesse. Hierbei handelt es sich um:

- Haushaltsführung
- Buchführung
- Prüfung des Zahlungsverkehrs
- Controlling und Revision

3.4 Referenzarchitektur

Zur Umsetzung der Leistungs- und Unterstützungsprozesse werden Anwendungen, IT- und Netzwerke, Gebäude, sowie Räume benötigt. Die nachfolgende Tabelle 6 stellt dies dar.

Anwendungen	IT-Systeme	Netze und Kommunikationsverbindungen	Gebäude und Räume
<ul style="list-style-type: none"> • Betriebssystem Windows • Verzeichnisdienst • Mailserver • Web-Browser • MS Office • Steuerfachverfahren • Vocario • AIS 	<ul style="list-style-type: none"> • Dateiserver • Steuerclient fest • Steuerclient mobil • TK-Anlage • Telefon • Faxgerät • DECT-Telefonie • Multifunktionsgerät • Lokale Drucker • Mobiler Drucker 	<ul style="list-style-type: none"> • Gebäudeverkabelung • ITN-XT • ITN-LSA • Inhouse-LAN 	<ul style="list-style-type: none"> • Gebäudekubator • Büroraum • Serverraum • Verteilerraum • Besprechungsraum • Drucker- und Kopierraum (Multifunktionsraum) • Aktenarchiv

Anwendungen	IT-Systeme	Netze und Kommunikationsverbindungen	Gebäude und Räume
<ul style="list-style-type: none"> PROMIS 	<ul style="list-style-type: none"> Scanner Wechseldatenträger 		<ul style="list-style-type: none"> Poststelle Telearbeitsplatz Sicherheitstechnik

Tabelle 6: Zielobjekte

Die Anwendungen und Clients werden zentral durch den zentralen IT-Dienstleister bereitgestellt. Demnach erfolgt eine bedarfsgerechte Abgrenzung gemäß Abbildung 6.

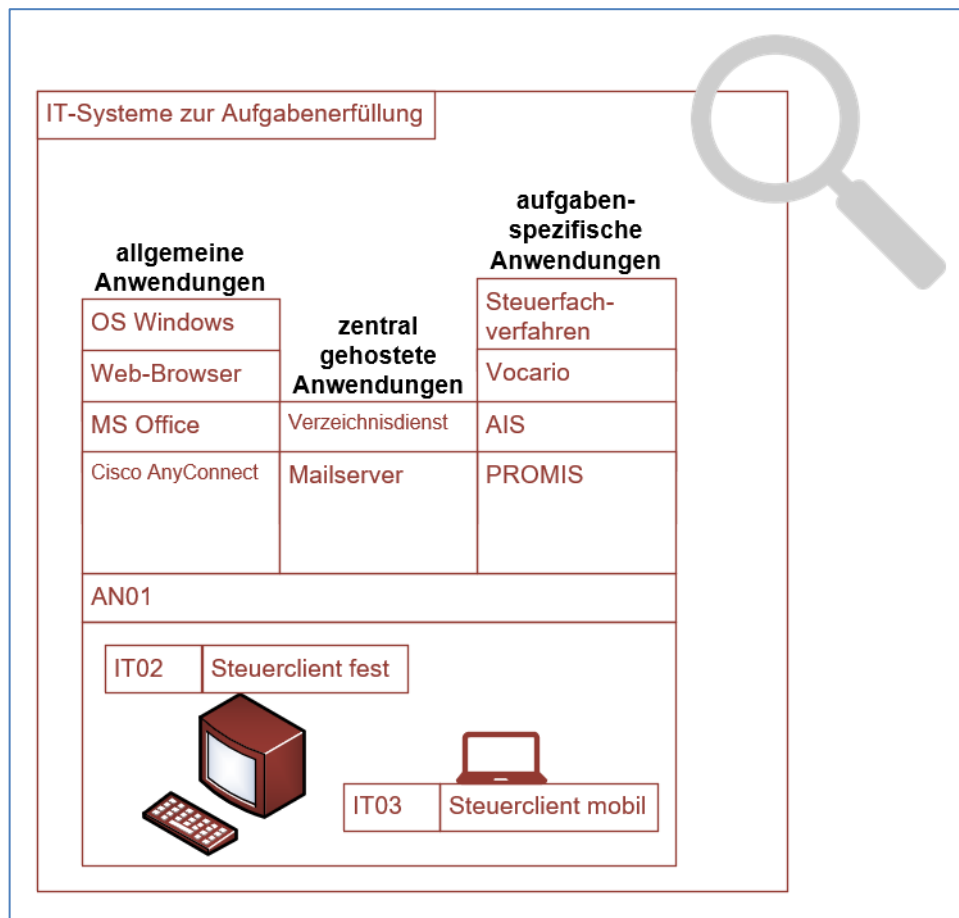


Abbildung 6: Abgrenzung der Anwendungen

3.5 Netzplan

Nachfolgend erfolgt die Darstellung der identifizierten Zielobjekte aus der Referenzarchitektur in Form eines Netzplans.

Dabei werden auch die Schnittstellen zu angrenzenden Informationsverbünden und Dienstleistern dargestellt.

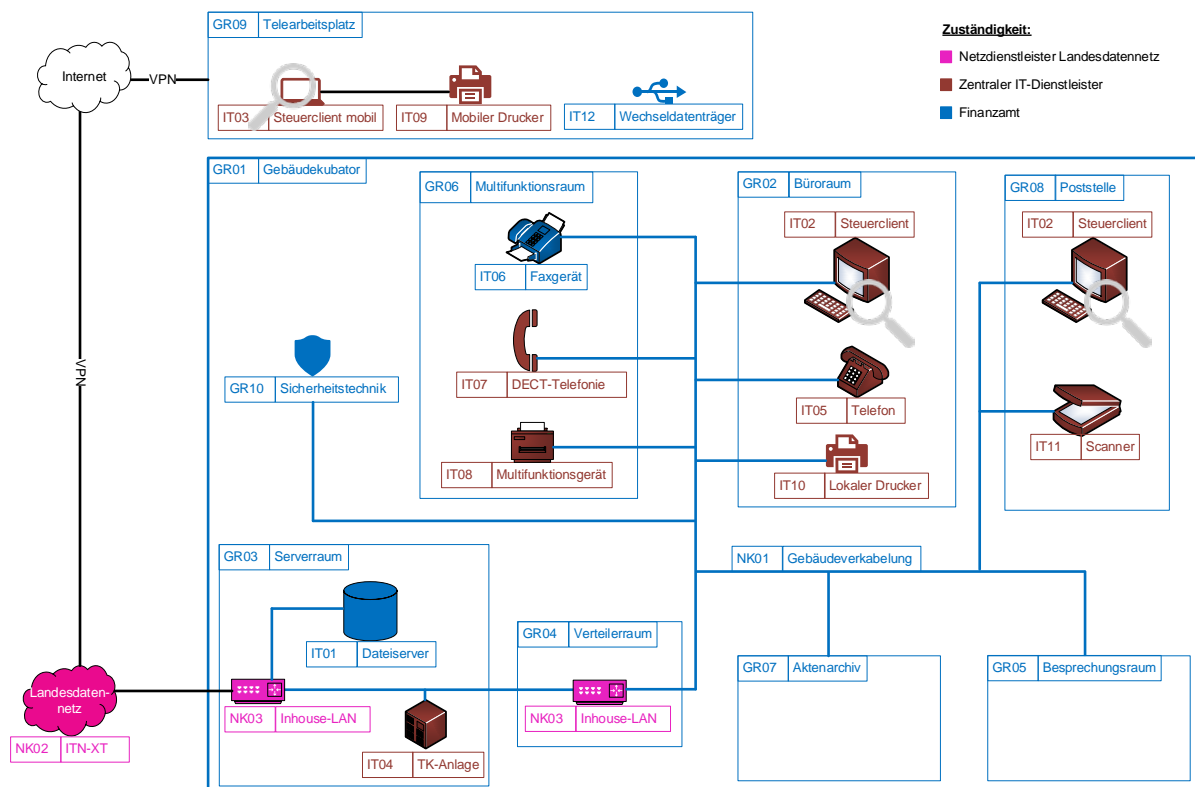


Abbildung 7: Netzplan

Der Netzplan ist in größerer Form in Anlage 1 beigelegt.

4 Schutzbedarfsfeststellung

Die Schutzbedarfsfeststellung richtet sich nach den Schutzbedarfen der verarbeiteten Informationen in den leistungserbringenden Geschäftsprozessen der Einnahmeverwaltung. Die Informationen werden durch die Anwendung „Steuerfachverfahren“ auf dem IT-System „Steuerclient“ verarbeitet. Das IT-System „Steuerclient“ wird in einem FA betrieben und genutzt.

Gemäß [Ref. 01] sind seitens des ISMS folgende Schutzziele verbindlich definiert und werden vollumfänglich berücksichtigt:

- Vertraulichkeit (confidentiality – C),
- Integrität (integrity – I) und
- Verfügbarkeit (availability – A).

Der Schutzbedarf für die Einnahmeverwaltung und demnach für den betrachteten Informationsverbund wird durch Vererbung des Schutzbedarfs des Steuerclients (vgl. [Ref. 07]) und des Steuerfachverfahrens (vgl. [Ref. 08]) bestimmt und führt zu:

- **Vertraulichkeit: hoch**
- **Integrität: hoch**
- **Verfügbarkeit: hoch**

Der Schutzbedarf vererbt sich durch das Maximumprinzip. Die Einnahmeverwaltung ist zur Durchführung ihrer Leistungsprozesse auf das Steuerfachverfahren und den Steuerclient angewiesen. Die Anwendungen werden durch die Unterstützungsprozesse und damit in Zusammenhang stehenden Zielobjekten orchestriert. Der Schutzbedarf der Einnahmeverwaltung muss sich demnach aus dem Steuerfachverfahren und dem Steuerclient bestimmen.

Die Schutzbedarfskategorien definieren sich nach der Richtlinie Risikomanagement (vgl. [Ref. 02]) im Ministerium der Finanzen.

Die Schutzbedarfsfeststellung ist für die verbindliche Anwendung in A.2 zu finden.

5 Modellierung

Die Informationsverbünde der Einnahmeverwaltung sind Teil des ISMS des MF ST. Der jeweilige Informationsverbund wendet die Vorgaben und Regularien des ISMS an und bringt diese im Informationsverbund zur Anwendung.

Grundsätze, Richtlinien und (Handlungs-) Anweisungen werden durch die übergeordnete Stelle und den ISB MF ST vorgegeben, gesteuert und auf Einhaltung kontrolliert. Die Umsetzung ist in der Einnahmeverwaltung sicherzustellen. Übergreifende Regelungen sind umzusetzen. Für die Einnahmeverwaltung werden dabei u. a. die Regelung zum Löschen und Vernichten, zu mobilen Endgeräten, zum Berichtswesen, zu Korrektur- und Vorbeugemaßnahmen, zur Detektion und Behandlung von Sicherheitsvorfällen, zur Organisation, zur Schulung und Sensibilisierung, zu Schwachstellen, zur Beschaffung und zum Outsourcing und zur Revision betrachtet. Innerhalb der Modellierung ist hierauf zu referenzieren, sofern es Relevanz für die identifizierten Zielobjekte besitzt.

Die Verantwortung für die Umsetzung der Regelungen liegt in der Hoheit des Bereichs-ISB; die Kontrolle der Umsetzung erfolgt durch den ISB des MF ST.

Die Modellierung stellt die identifizierten Zielobjekte, die in den Zuständigkeits- und Verantwortungsbereich des Finanzamts fallen, dar. Hierbei kann ein Zielobjekt durch einen oder mehrere Bausteine beschrieben werden.

Die Modellierung ist in A.3 zu finden.

6 Zu erfüllende Anforderungen und umzusetzende Maßnahmen

Für die modellierten Bausteine sind grundsätzlich alle Anforderungen zu erfüllen. Hierbei erfolgt folgende Differenzierung:

- BASIS-Anforderungen müssen erfüllt werden. Die getroffenen Maßnahmen müssen eindeutig und nachvollziehbar dokumentiert sein.
- STANDARD-Anforderungen können erfüllt werden. Werden diese nicht erfüllt, so ist eine Risikoanalyse durchzuführen. Die getroffenen Maßnahmen sind eindeutig und nachvollziehbar zu dokumentieren. Bei Standard-Anforderungen kann es Teilanforderung geben, die MUSS-Anforderungen sind; diese müssen demnach auch erfüllt werden.
- Anforderungen bei ERHÖHTEM Schutzbedarf dienen zur Orientierung. Aufgrund des Schutzbedarfs wird eine Risikoanalyse gefertigt. Die getroffenen Maßnahmen sind eindeutig und nachvollziehbar zu dokumentieren.

Abgesehen vom grundschutzkonformen Vorgehen treffen nicht alle Anforderungen aus den modellierten Bausteinen auf die identifizierten Zielobjekte zu. Diese Anforderungen müssen demnach nicht betrachtet werden. Der pauschale Ausschluss mit Begründung ist in nachfolgenden Kapiteln zu finden. Ist keine Maßnahme für eine zutreffende Anforderung etabliert oder möglich, wird eine Risikoanalyse mit einer Restrisikobetrachtung durchgeführt (vgl. Kap. 7). Ausgenommen davon sind zu Teilen Anforderungen für erhöhten Schutzbedarf für die Ersatzmaßnahmen getroffen werden können. Das ermöglicht, dass in der Betrachtung der Bausteine einzelne Anforderungen an anderer Stelle betrachtet werden.

Die Referenzierung der zu betrachtenden Zielobjekte erfolgt mittels Modellierung gemäß A.3.

6.1 Ausgeschlossene und an anderen Stellen bearbeitete Anforderungen aus Bausteinen

Im Rahmen der Modellierung (vgl. A.3) sind die relevanten Bausteine identifiziert und zur Anwendung gebracht worden.

Das Herstellen eines einheitlichen Sicherheitsniveaus ist nur mit einem übergeordneten ISMS möglich, welches einheitliche Vorgaben für die Anwendung und Umsetzung von Bausteinen macht. Einzelne Bausteine oder Anforderungen in Bausteinen können für entbehrlich betrachtet werden. Die Entbehrlichkeit lässt sich an dieser Stelle wie folgt begründen:

- Die Anforderung oder der Baustein kommt in der Einnahmeverwaltung nicht zum Tragen.
- Das Zielobjekt ist nicht Teil des Informationsverbunds.
- Die Anforderung wird in einem anderen Informationsverbund oder durch einen Dienstleister betrachtet und bewertet.

Die notwendigen Begründungen hierfür werden in den nachfolgenden Teilkapiteln dargestellt. Der Ausschluss von (dedizierten) Anforderungen, insbesondere für Anforderungen aus Bausteinen, die zur Anwendung kommen, erfolgt in A.4.

Einzelne Bausteine kommen im Rahmen der Modellierung (vgl. A.3) teilweise mehrfach zur Anwendung. Dies ist notwendig um die spezifischen Zielobjekte hinreichend genau zu modellieren. In einzelnen Zielobjekten können hierbei Anforderungen ausgeschlossen werden, die bei anderen Zielobjekten

wieder zur Anwendung kommen können. Die Notwendigkeit dessen ist im Rahmen der Anwendung des IT-Grundschutz-Profiles (vgl. A.4) konkretisiert.

6.2 Ausgeschlossene oder an anderer Stelle bearbeitete Anforderungen aus IT-Systemen

In den nachfolgenden Teilkapiteln werden Anforderungen dargestellt, die an anderer Stelle bearbeitet und betrachtet werden. Dies umfasst entweder die Verantwortung anderer Betreiber oder die Zuordnung in einem anderen Informationsverbund.

6.2.1 Zielobjekt IT03

Anforderung	Bezeichnung	Typ	Bemerkung
SYS.3.1.A3	Einsatz von Personal Firewalls	Basis	Dies wird im Sicherheitskonzept des Steuerclients geregelt.
SYS.3.1.A9	Sicherer Fernzugriff mit Laptops	Basis	Dies wird im Sicherheitskonzept des Steuerclients geregelt.

Tabelle 7: Anforderungen des Zielobjekts IT03

6.2.2 Zielobjekt IT04

Anforderung	Bezeichnung	Typ	Bemerkung
NET.4.1.A1	Anforderungsanalyse und Planung für TK-Anlagen	Basis	Die TK-Anlage an sich wird durch einen Dienstleister bereitgestellt. Dieser ist für die Zulieferung und die sicherheitstechnische Betrachtung zuständig. Die Betreiberverantwortung liegt beim Dienstleister. Die Kontrollpflicht obliegt dem Finanzamt.
NET.4.1.A2	Auswahl von TK-Diensteanbietern	Basis	
NET.4.1.A5	Protokollierung bei TK-Anlagen	Basis	
NET.4.1.A9	Schulung zur sicheren Nutzung von TK-Anlagen	Standard	
NET.4.1.A12	Datensicherung der Konfigurationsdateien	Standard	

Tabelle 8: Anforderungen des Zielobjekts IT04

6.2.3 Zielobjekt IT05

Das Finanzamt ist für die Beschaffung und Aufstellung des Zielobjekts IT05 Telefon selbst verantwortlich.

Anforderung	Bezeichnung	Typ	Bemerkung
NET.4.1.A1	Anforderungsanalyse und Planung für TK-Anlagen	Basis	Die TK-Anlage an sich wird durch einen Dienstleister bereitgestellt. Dieser ist für die Zulieferung und die sicherheitstechnische Betrachtung zuständig. Hierbei handelt es sich um das Zielobjekt IT04. Der hier angewandte Baustein fokussiert ausschließlich auf das Telefon in Büroarbeitsplätzen von Mitarbeitenden.
NET.4.1.A2	Auswahl von TK-Diensteanbietenden	Basis	
NET.4.1.A6	Erstellung einer Sicherheitsrichtlinie für TK-Anlagen	Standard	
NET.4.1.A7	Geeignete Aufstellung der TK-Anlage	Standard	
NET.4.1.A13	Beschaffung von TK-Anlagen	Standard	
NET.4.1.A14	Notfallvorsorge für TK-Anlagen	Standard	
NET.4.1.A15	Notrufe bei einem Ausfall der TK-Anlage	Standard	

Tabelle 9: Anforderungen des Zielobjekts IT05

6.2.4 Zielobjekt IT07

Das Finanzamt ist für die Beschaffung und Aufstellung des Zielobjekts IT07 DECT-Telefonie selbst verantwortlich.

Anforderung	Bezeichnung	Typ	Bemerkung
NET.4.1.A1	Anforderungsanalyse und Planung für TK-Anlagen	Basis	Die TK-Anlage an sich wird durch einen Dienstleister bereitgestellt. Dieser ist für die Zulieferung und die sicherheitstechnische Betrachtung zuständig. Hierbei handelt es sich um das Zielobjekt IT04. Der hier angewandte Baustein fokussiert ausschließlich auf das Telefon in Büroarbeitsplätzen von Mitarbeitenden.
NET.4.1.A2	Auswahl von TK-Diensteanbietenden	Basis	
NET.4.1.A6	Erstellung einer Sicherheitsrichtlinie für TK-Anlagen	Standard	
NET.4.1.A7	Geeignete Aufstellung der TK-Anlage	Standard	
NET.4.1.A13	Beschaffung von TK-Anlagen	Standard	
NET.4.1.A14	Notfallvorsorge für TK-Anlagen	Standard	
NET.4.1.A15	Notrufe bei einem Ausfall der TK-Anlage	Standard	

Tabelle 10: Anforderungen des Zielobjekts IT07

6.2.5 Zielobjekt IT08, IT09, IT10 und IT11

Die Drucker werden durch den Dienstleister zentral bereitgestellt und betrieben. Für die Beschaffung und die Aufstellung ist das Finanzamt zuständig.

Anforderung	Bezeichnung	Typ	Bemerkung
SYS.4.1.A7	Beschränkung der administrativen Fernzugriffe auf Drucker, Kopierer und Multifunktionsgeräte	Standard	Die Drucker werden nach Vorgaben des Ministeriums der Finanzen beschafft. Die Nutzung erfolgt im Finanzamt. Der Betrieb erfolgt durch den Dienstleister und nach den abgestimmten Vereinbarungen.
SYS.4.1.A15	Verschlüsselung von Informationen bei Druckern, Kopierern und Multifunktionsgeräten	Standard	
SYS.4.1.A17	Schutz von Nutz- und Metadaten	Standard	
SYS.4.1.A18	Konfiguration von Druckern, Kopierern und Multifunktionsgeräten	Standard	

Tabelle 11: Anforderungen der Zielobjekte IT08, IT09, IT10 und IT11

7 Risikoanalyse

Im Anschluss an den IT-Grundschutz-Check ist eine Risikoanalyse durchzuführen. Hierbei erfolgt eine zweistufige Analyseform:

- Für **nicht** oder nur **teilweise erfüllbare Anforderungen** im Rahmen von modellierten Bausteinen ist eine Risikobewertung für diese Anforderung vorzunehmen. Die Einschätzung richtet sich gemäß den Vorgaben aus [Ref. 02].

Die Zuständigkeit für diese Risikoanalysen unterscheidet sich:

- Ministerium der Finanzen:
Für übergreifende Anforderungen aus den ISMS.1- und Prozessbausteine.
- Bereichs-ISB des Finanzamts:
Für Anforderungen aus der Modellierung der Zielobjekte.
- Aufgrund des identifizierten Schutzbedarfs ist eine Risikoanalyse für den Informationsverbund notwendig. Hierfür wird eine Vorlage seitens des Ministeriums für Finanzen bereitgestellt. Diese Vorlage ist in Abstimmung mit dem ISB MF ST zu erweitern, sofern es Abweichungen zu den hier definierten Standards gibt.

Die Vorlage wird durch A.5 bereitgestellt.

Die Ergebnisse der Risikoanalysen sind zu dokumentieren und regelmäßig auf Aktualität und Angemessenheit zu prüfen.

8 Anwendungshinweise

8.1 Allgemeines

Das IT-Grundschutz-Profil beschreibt ein idealtypisches Finanzamt im Bundesland Sachsen-Anhalt und stellt alle allgemeingültigen Grundsätze dar. Aufgrund der Einbettung in den Geschäftsbereich des MF ST existieren verteilte Zuständigkeiten und Verantwortungen (vgl. Kap. 1.5). Für die Anwendung ist eine Verantwortungsmatrix in Anlage 2 beigelegt.

8.2 Implementierung

Zur Anwendung dieses IT-Grundschutz-Profiles sind durch die Amtsleitung die notwendigen organisatorischen und technischen Maßnahmen zu treffen. Aufgrund des zu erwartenden Aufwands bei der Anwendung des IT-Grundschutz-Profiles ist eine gestaffelte Umsetzung zulässig.

Diese stellt sich so dar, dass es für die erstmalige Anwendung des IT-Grundschutz-Profiles zulässig ist, dass die Umsetzung gemäß Basis-Absicherung zur Umsetzung kommt. Diese Umsetzung ist befristet für ein Jahr. Nach einem Jahr und demnach bei der jährlichen Überprüfung muss die Standard-Absicherung zur Anwendung kommen. Es empfiehlt sich, dass bei der erstmaligen Anwendung auch die Standard-Anforderungen geprüft werden und sich mit den allgemeinen und spezifischen Risiken vertraut gemacht wird.

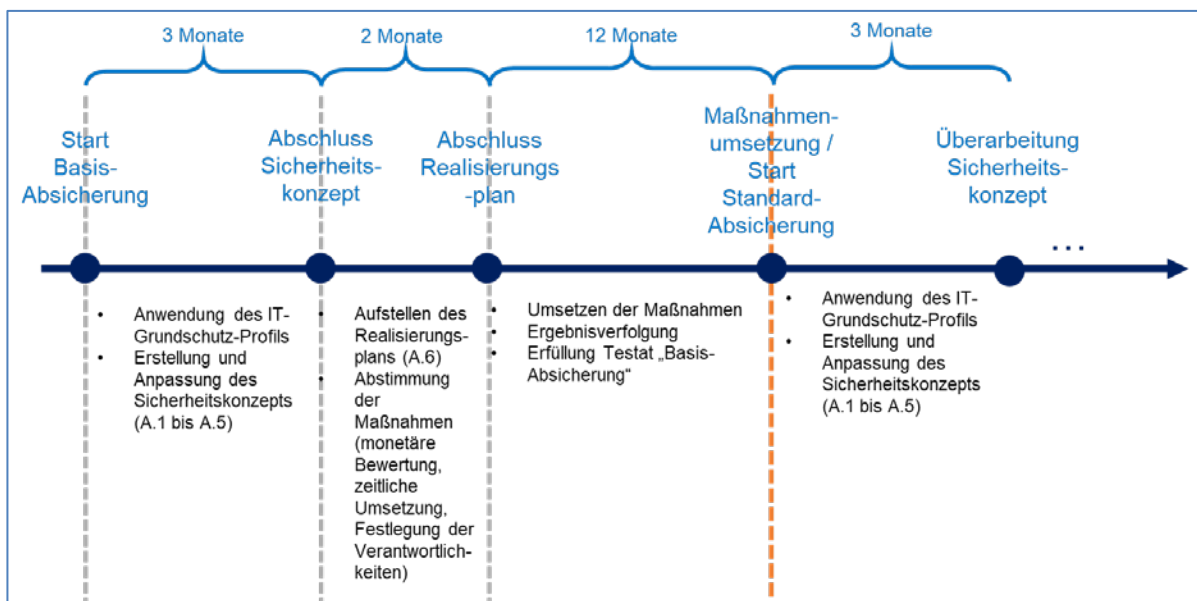


Abbildung 8: Zeitliche Umsetzung des IT-Grundschutz-Profiles

Ziel des Profils ist ein einheitliches Schutzniveau durch die Standard-Absicherung zu erreichen. Der Zwischenschritt der Basis-Absicherung dient der Sensibilisierung für die Komplexität der Informationssicherheit. Die Anwendung des IT-Grundschutz-Profiles verfolgt zusätzlich das Ziel, eine Zertifizierungsfähigkeit herzustellen.

Zur Nachweisführung und Ablage der Referenzdokumente kommen die etablierten IT-Systeme im Geschäftsbereich des MF ST zum Einsatz. Ab der Standard-Absicherung muss das vorgegebene IT-Grundschutz-Tool genutzt werden.

8.3 Weiterentwicklung

Das IT-Grundschutz-Kompendium des BSI wird jährlich aktualisiert. Bei Veröffentlichung ist durch den ISB MF ST eine Prüfung hinsichtlich der Anwendbarkeit neuer Bausteine vorzunehmen. Gleichzeitig ist zu prüfen, inwiefern sich bestehende und zum Einsatz kommende Bausteine geändert haben.

Der Einsatz weiterer branchenspezifischer Standards ist zu prüfen. Hierbei empfiehlt sich insbesondere der Sicherungsleitfaden Perimeter des Verbands der Sicherheitstechnik².

Bei der zweijährlichen Revision (vgl. Kap. 1.7) ist die Anwendbarkeit des IT-Grundschutz-Profils weiter zu prüfen und gegebenenfalls haben Anpassungen zu erfolgen. Sobald eine Anpassung des Profils resultiert, muss ein erneuter IT-Grundschutz-Check erfolgen; die Risikoanalyse folgt dementsprechend.

² vgl. https://vds.de/fileadmin/Website_Content/Images/VdS_Publikationen/vds_3143_web.pdf [Stand: 20.03.2023]

9 Abkürzungen

Kürzel	Erklärung
BLSA	Bau- und Liegenschaftsmanagement Sachsen-Anhalt
FA	Finanzamt
GSC	IT-Grundschutz-Check
ISB	Informationssicherheitsbeauftragte/r
ISMS	Informationssicherheitsmanagementsystem
MF ST	Ministerium der Finanzen Sachsen-Anhalt

Tabelle 12: Abkürzungen

10 Referenzen

Die Ablage der Dokumente erfolgt elektronisch im DMS des AG InfoSic.

Im Dokument referenzierte Dokumente sind dort mit Ergebnis- und Begleitdokumenten unter ihrer jeweiligen Dokumenten-ID als Ordner abgelegt.

Ref.-Nr.	Bezeichnung	Bemerkung
[Ref. 01]	Leitlinie zur Gewährleistung der Informationssicherheit	Leitlinie des Ministeriums der Finanzen
[Ref. 02]	Richtlinie Risikomanagement, V1.0	Richtlinie zum Risikomanagement mit Risikokategorien, Vorlage zur Risikoanalyse
[Ref. 03]	Organisationsrichtlinie, V1.0	Struktur und Aufbau der ISMS-Organisation im Geschäftsbereich des Ministeriums der Finanzen mit Rollensteckbriefen
[Ref. 04]	Auditierungsschema, V 2.3	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Zertifikat/ISO27001/Auditierungsschema_Kompendum.pdf?__blob=publicationFile&v=1 [Stand 20.03.2023]
[Ref.05]	Liste der Referenzdokumente zum Auditbericht, Version 2.0	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Zertifikat/ISO27001/Liste_Referenzdokumente_Auditbericht_Kompendum.xlsx?__blob=publicationFile&v=1 [Stand 20.03.2023]
[Ref. 06]	BSI-Standard 200-2	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.pdf?__blob=publicationFile&v=2 [Stand 20.03.2023]
[Ref. 07]	Schutzbedarfsfeststellung Steuerclient	A.2 Schutzbedarfsfeststellung Steuer-Client 3.0 vom 18.08.2020
[Ref. 08]	Schutzbedarfsfeststellung Steuerfachverfahren	A.2 Schutzbedarfsfeststellung Steuerverfahren vom 11.09.2019

Tabelle 13: Referenzen

11 Anlagen

Die Ablage der Dokumente erfolgt elektronisch im DMS des AG InfoSic.

Die in diesem Dokument referenzierten Anlagen sind unter ihrer jeweiligen Dokumenten-ID als Ordner abgelegt.

Anlagen-Nr.	Dokumenten-ID	Dokumententitel
[Anl. 01]		Abbildungen aus dem IT-Grundschutz-Profil
[Anl. 02]		Verantwortlichkeitsmatrix

Tabelle 14: Anlagen