IT-Grundschutz des Bundes

Überprüfung der Vorgaben des Bundes für den IT-Grundschutz

Dokumentenname	IG - Bericht Überprüfung IT-Grundschutz Bund V1.0.docx
Version	1.0
Erstellt am	10.01.2025
Aktenzeichen	SEPOS-330-Grundlagen/10/6/1

1 EINLEITUNG

1.1 Sinn und Zweck des IT-Grundschutzes Bund

Der IT-Grundschutz des Bundes ist ein wesentlicher Bestandteil der Cybersicherheit in der Schweizer Bundesverwaltung und der Armee. Der IT-Grundschutz Bund ist zunächst eine Methode: Für alle Informatikmittel und Datensammlungen (Schutzobjekte), die für die Aufgabenerfüllung der Bundesbehörden nicht besonders kritisch sind oder keine sensiblen Daten enthalten, soll die Einhaltung einer Reihe vordefinierter und standardisierter Sicherheitsanforderungen genügen, um eine hinreichende Sicherheit zu gewährleisten – ohne zusätzliche, aufwändige Massnahmen. Für kritischere Systeme und Daten reichen diese Mindestanforderungen in der Regel jedoch nicht aus. In solchen Fällen muss die zuständige Stelle eine Risikoanalyse durchführen und darauf gestützt ein Informationssicherheits- und Datenschutzkonzept (*ISDS-Konzept*) erstellen. Der Begriff «IT-Grundschutz Bund» wird dann auch für den verbindlichen Katalog der minimalen Informationssicherheitsanforderungen, die alle Schutzobjekte erfüllen müssen, verwendet.

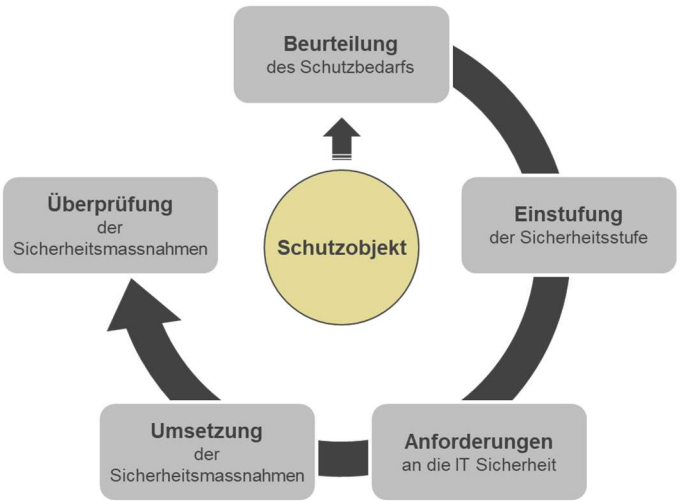

Abbildung 1: Sicherheitsverfahren

Das Sicherheitsverfahren (vgl. Abbildung 1) bildet zusammen mit den wesentlichen Gesetzen, Verordnungen, Weisungen und Richtlinien (vgl. Abbildung 2**Abbildung 2:** IT-Sicherheitsgrundlagen) die massgeblichen Elemente des Rahmenwerks zum IT-Grundschutz Bund.

Abbildung 2: IT-Sicherheitsgrundlagen

Die Schutzbedarfsanalyse dient der Evaluierung des Schutzbedarfs von Schutzobjekten in Bezug auf Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit sowie das Einhalten von rechtlichen Vorgaben zum Schutz von Informationen und Daten (z.B. Datenschutzgesetz). Der IT-Grundschutz definiert die minimalen organisatorischen, personellen und technischen Anforderungen und Massnahmen für alle Schutzobjekte. Diese Vorgaben basieren auf den in Abbildung 2 dargestellten IT-Sicherheitsgrundlagen.

Für Schutzobjekte mit höherer Sicherheitsstufe gelten die Mindestanforderungen des IT-Grundschutzes sowie weiterführende Anforderungen aus der Risikoanalyse und den dafür relevanten Rechtsgrundlagen (z.B. Datenschutz oder Schutz klassifizierter Informationen).

1.2 Prüfauftrag, Prüfmethoden und Vorgehen

Die Anforderungen seitens Auftraggeber SEPOS wurden folgendermassen formuliert:

«Am 1. Mai 2024 hat der Bundesrat von den Lehren aus dem Vorfall XPlain AG Kenntnis genommen und in der Folge Massnahmen beschlossen, um die Sicherheit bei der Zusammenarbeit mit externen Dienstleistern zu verbessern. Eine Voraussetzung dafür ist, dass die Vorgaben des Bundes zur Informationssicherheit aktuell und wirksam, aber auch für Dienstleister in der Praxis umsetzbar sind. Der Bundesrat hat deshalb das VBS (Staatssekretariat für Sicherheitspolitik, SEPOS) beauftragt, den IT-Grundschutz des Bundes zu überprüfen und ihn bis Ende 2024 über den Anpassungsbedarf zu informieren.»

Die InfoGuard AG wurde als externer Leistungserbringer damit beauftragt, den bestehenden IT-Grundschutz zu evaluieren. Ziel dieser Evaluation ist es, die Aktualität, Vollständigkeit, Wirksamkeit und praktische Umsetzbarkeit zu überprüfen. Dafür wurden folgende Leistungen verlangt:

1. **Unabhängige Beurteilung der bestehenden Vorgaben und Hilfsmittel** zum IT-Grundschutz unter Berücksichtigung des internationalen Standards für Informationssicherheit ISO/IEC 27001:2022 sowie von Best Practices durch die InfoGuard AG.
2. **Befragung der Bundesstellen, Kantonen und (externen) Dienstleistern** zur praktischen Umsetzbarkeit sowie zu weiteren Erfahrungen und Herausforderungen mit dem IT-Grundschutz mithilfe von Fragebogen und Interviews.
3. **Erarbeitung des Revisionsbedarfs und von Lösungsvorschlägen** basierend auf den durch die Beurteilung und Befragung gewonnenen Erkenntnissen.

Die Evaluation des IT-Grundschutzes wurde gemäss folgendem Vorgehen durchgeführt:

Abbildung 3: Vorgehen zur Beurteilung der IT-Grundschutz-Vorgaben

1.3 Terminologie

In den Vorgabendokumenten wird der Begriff «IT-Grundschutz» noch nicht konsistent verwendet. Insbesondere in älteren Dokumenten finden sich noch die Begriffe «IKT-Grundschutz» oder nur «Grundschutz». Zum besseren Verständnis wird in diesem Bericht für die Beschreibung der Vorgabensammlung für die unterste Informationssicherheitsstufe des Bundes durchgehend der Begriff «IT-Grundschutz» verwendet.

2 BEURTEILUNG DER IT-GRUNDSCHUTZ-VORGABEN DURCH INFOGUARD AG

Im Kern der Überprüfung durch InfoGuard AG stand die Sicherheitsvorgabe Si001 «IT-Grundschutz in der Bundesverwaltung» des Bundesamts für Cybersicherheit (BACS). Es wurden fünfzehn weitere dazugehörige Hilfsmittel und damit verbundenen Vorgaben des BACS analysiert und bewertet (vgl. Kapitel 0).

2.1 Allgemeines

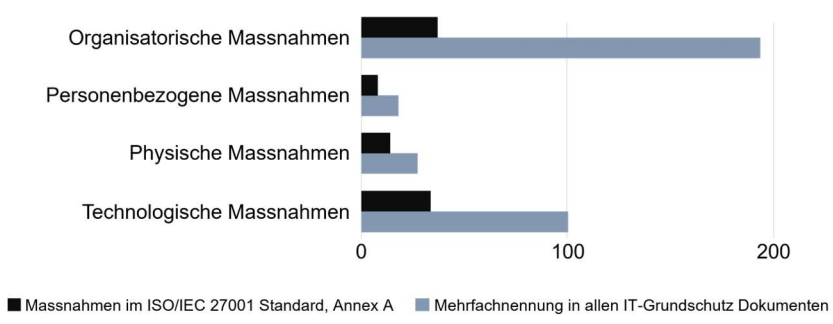

Abbildung 4: Mehrfachnennung der ISO/IEC 27001:2022 Massnahmen über alle IT-Grundschutz-Dokumente

Im Rahmen der Beurteilung wurden alle zur Verfügung gestellten Vorgaben und Hilfsmittel dem Standard ISO/IEC 27001:2022 und dessen Massnahmen in Annex A gegenübergestellt. Dabei zeigte sich, dass insbesondere die organisatorischen und technologischen Massnahmen des ISO/IEC 27001-Katalogs mehrfach genannt werden (vgl. Abbildung 4).

Die Mehrfachnennungen von Vorgaben, beispielsweise im Hinblick auf Verantwortlichkeiten, erstrecken sich über die Mehrheit der analysierten Dokumente. Dabei umfassten die Vorgaben des IT-Grundschutzes, die als «Nennung» einer ISO/IEC Massnahme bewertet wurden, nicht immer die klassische Beschreibung einer Anforderung, wie sie in der Sicherheitsvorgabe Si001 dargestellt ist. Vielmehr beinhalten sie auch Anweisungen, Hinweise, oder vergleichbare Elemente, die in den beurteilten Dokumenten gefunden wurden.

Die Mehrfachnennung einer Massnahme birgt das Risiko für missverständliche oder fehlerhafte Definitionen oder kann zu unterschiedlichen Interpretationen einer Massnahme führen. Bei einer Mehrzahl von unterschiedlichen Beschreibungen ist auch unklar ist, welche der Definitionen nun Gültigkeit hat.

Mit der Sicherheitsvorgabe Si001 besteht ein Katalog, welcher die Massnahmen klar und eindeutig beschreiben soll, und demnach als einzige Referenz genutzt werden sollte. Die Ursache für die vielen Nennungen konnte nicht ermittelt werden. Eine mögliche Erklärung ist das organische Wachstum, ausgelöst durch die regelmässige Aktualisierung und Verfeinerung der Vorgaben durch verschiedene Stellen, wodurch die ISO/IEC 27001-Massnahmen über eine Vielzahl unterschiedlicher Dokumente hinweg verteilt wurden.

Ein wichtiger Aspekt, der alle Sicherheitsstufen betrifft, ist die Einbettung der Anforderungen in ein übergeordnetes Rahmenwerk, welches der Informationssicherheit einen klaren Rahmen gibt. Bei der Überprüfung aller Dokumente fiel auf, dass es für die Adressaten oft schwierig ist, die Dokumente, Verfahren und Methoden einzuordnen und entsprechend den organisatorischen Gegebenheiten umzusetzen (siehe nachfolgende Erläuterungen). Dasselbe gilt auch für die Abgrenzung zwischen den einzelnen Sicherheitsstufen. Ein gut strukturierter und systematischer Ansatz, der den Adressaten Orientierung bietet, würde erheblich zur Verständlichkeit und Umsetzbarkeit beitragen.

2.2 Sicherheitsvorgabe Si001 – IT-Grundschutz in der Bundesverwaltung

Die Sicherheitsvorgabe «Si001 – IT-Grundschutz in der Bundesverwaltung» vom 5. Juli 2024 wurde einer vertieften Beurteilung bezüglich Aktualität, Vollständigkeit, Wirksamkeit und praktischer Umsetzbarkeit unterzogen.

Die Sicherheitsvorgabe Si001 ist bezüglich ISG/ISV auf einem aktuellen Stand, erfordert jedoch inhaltliche Anpassungen im Hinblick auf die Abdeckung (Scope) und die Qualität der Beschreibung von Anforderungen.

Der Aufbau und die Struktur der Vorgaben entsprechen dem Grundgedanken von Standards wie ISO/IEC 27001:2022. Dieser empfiehlt, nicht nur risikomindernde Massnahmen strukturiert, umfassend und systematisch zu definieren, umzusetzen und zu überprüfen, sondern auch ein wiederkehrendes Verfahren zu etablieren, um den Gesamtschutz einer Organisation gegen Informationssicherheitsbedrohungen mittels eines geeigneten Informationssicherheitsmanagementsystems (ISMS) sicherzustellen.

Die Grundsätze und Prinzipen entsprechen insgesamt den Erwartungen an einen IT-Grundschutz. Neuere Sicherheitskonzepte wie Cloud-Sicherheit oder Zero Trust werden aber in den Sicherheitsabforderungen nicht hinreichend behandelt.

Die Qualität der einzelnen Sicherheitsanforderungen variiert stark hinsichtlich der Terminologie, ihrer Verständlichkeit, ihres Detailierungsgrads, ihrer Anwendbarkeit und ihrer praktischen Umsetzbarkeit. Häufig sind die Ziele (das «Was») und die Umsetzung (das «Wie») nicht klar voneinander abgegrenzt. Dadurch können die Anforderungen – abhängig vom jeweiligen Adressaten - teilweise schwer fassbar und verständlich werden, was sich in einer herausfordernden Umsetzung der Massnahmen niederschlägt.

Im Gegensatz zur Mehrfachnennung von Vorgaben über alle Dokumente (vgl. Abbildung 5) ergibt sich bei der Einzelbetrachtung der Sicherheitsvorgabe Si001 ein anderes Bild:

Die Abdeckung gegenüber ISO 27001:2022 (Annex A) zeigt in einigen Bereichen Lücken auf und bestätigt den Bedarf, bestimmte Themen umfassender abzudecken oder zu ergänzen (vgl. Abbildung 5).

Nachfolgend sind die Themen, die in der Sicherheitsvorgabe Si001 besser abgedeckt werden sollten, zusammengefasst:

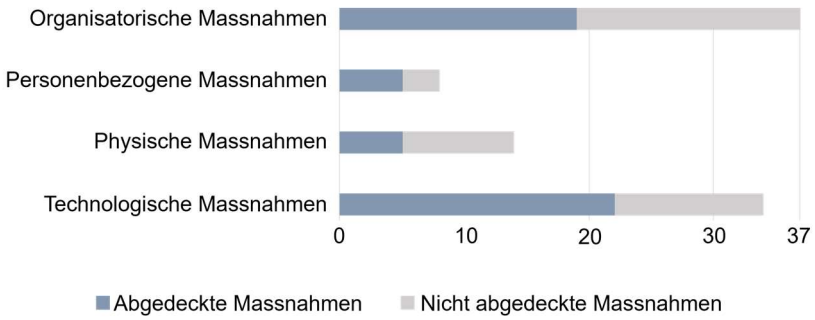

Abbildung 5: Abdeckung der Anforderungen des ISO/IEC 27001:2022-Standards durch die Sicherheitsvorgabe Si001

Themen, welche	
…angepasst oder erweitert werden sollten	**...fehlen**
Lieferketten (Third Party Risk Management)	Datenschutz
Vorfallmanagement	Überwachung und Bedrohungserkennung
Wiederherstellbarkeit	Testen von Software
Kryptographische Verschlüsselung	Künstliche Intelligenz
Vorgaben zu Cloud-Nutzung	
Zero Trust	

2.3 IT-Grundschutz in der Bundesverwaltung – Unterstützende Dokumente

Zusätzlich zur Sicherheitsvorgabe Si001 wurden weitere fünfzehn Dokumente analysiert (vgl. Anhang zum Bericht). Für die folgenden drei Dokumente erfolgte ebenfalls eine vertiefte Prüfung:

- **Sicherheitsvorgabe Si004 - Regelung der Zugriffe auf Ressourcen im Internet: Web Proxy Richtlinie BV**, Version 1.3, Stand 15.12.2020: Das Dokument enthält sinnvolle Vorgaben, die insbesondere im Bereich der technischen Vorgaben vertieft werden sollten. Eine neue Version wird benötigt, um rechtlichen Anpassungen und dem technischen Fortschritt gerecht zu werden.
- **SB003 - Malwareschutz Strategie in der Bundesverwaltung**, Version 5.0, Stand 01.09.2021: Die Vorgaben sind teilweise lückenhaft und weisen einen hohen Interpretationsspielraum auf.
- **Sicherheitsvorgabe P042 - Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept)**, Version 4.5, Stand 07.09.2023: Die Vorgaben sind sehr grob beschrieben und die Strukturierung ist anspruchsvoll. Zudem fehlen Hilfestellungen, wie die Vorgaben zu überprüfen sind.

2.4 Schlussfolgerungen

In der Gesamtsicht ergaben sich grosse Unterschiede in der Beurteilung der verschiedenen Vorgaben. Die hervorgehobenen Dokumente schnitten jedoch im Durchschnitt etwas positiver ab als die Gesamtheit. Insgesamt lässt sich zu den analysierten Vorgaben und Hilfsmitteln Folgendes feststellen:

Aktualität

Zwei der überprüften Dokumente (Sicherheitsvorgabe Si001 und P041-Hi01-Schutzbedarfsanalyse) wurden nach Inkraftsetzung des ISG/ISV revidiert und berücksichtigen diese Regulatorien. Die übrigen zur Verfügung gestellten Dokumente wurden zwischen 2016 und 2023 erstellt und berücksichtigen daher das ISG/ISV nicht. Hinsichtlich des verwendeten Standards wird noch auf die veraltete Version ISO/IEC 27001:2013 verwiesen.

Vollständigkeit

Eine konkrete Abgrenzung und Zuweisung der Sicherheitsstufe, für die das Dokument gilt, ist nicht in jedem Fall ersichtlich. Die Abdeckung des Standards ISO/IEC 27001:2022 ist aus Sicht der InfoGuard AG noch nicht hinreichend.

Wirksamkeit (Kosten/Nutzen)

Der IT-Grundschutz des Bundes definiert als gemeinsamer Nenner die minimalen Anforderungen und gilt für alle Schutzobjekte, unabhängig von ihrer Art. Da aber in der Sicherheitsvorgabe Si001 nicht zwischen verschiedenen Arten differenziert wird, besteht das Risiko, dass sich die Anforderungen nicht mit derselben Wirksamkeit auf unterschiedliche Schutzobjektarten anwenden lassen.

Praktische Umsetzbarkeit

Ein transparenter Aufbau und eine übersichtliche Struktur der informationssicherheitsbezogenen Elemente (Prozesse, Vorgaben, Hilfsmittel etc.) sind nicht ersichtlich, was das Verständnis für den Adressaten erschwert. Aufgrund der mangelnden Praktikabilität und der fehlenden konkreten Zuweisung des Adressatenkreises ist es schwierig, die Vorgaben zielgerichtet anzuwenden. Zudem weist die Mehrheit der Dokumente Verbesserungspotenzial in Bezug auf Verständlichkeit, Präzision und Adressatengerechtigkeit auf.

3 BEFRAGUNG BUNDESSTELLEN, KANTONE UND (EXTERNEN) DIENSTLEISTER

Die **Umsetzbarkeit**, **Herausforderungen** und **Verbesserungsmassnahmen** des IT-Grundschutzes wurden mittels eines Fragebogens sowie ergänzenden Interviews erhoben. Der Fragebogen umfasste 25 Fragen mit Auswahlmöglichkeiten basierend auf einer vierstufigen Skala und einer Option für Freitext-Antworten. Zusätzlich wurde gezielt Feedback für jede Anforderung in der Sicherheitsvorgabe Si001 sowie zu einigen Hilfsmitteln des IT-Grundschutzes eingeholt. Der Fragebogen wurde an 29 Stellen der Bundesverwaltung, vier kantonale Stellen und sieben externe Dienstleister des Bundes versandt und erzielte eine **Rücklaufquote von 63%** (vgl. Abbildung 6).

Abbildung 6: Rücklaufquote Umfrage

Ergänzend dazu wurden Interviews mit drei kantonalen Stellen und drei externen Dienstleistern des Bundes geführt. Diese kombinierte Erhebung ermöglichte sowohl eine quantitative Analyse als auch die Einbeziehung qualitativen Feedbacks zu den IT-Grundschutz-Vorgaben und den unterstützenden Dokumenten.

3.1 Zusammenfassende Beurteilung über alle befragten Organisationen

Der IT-Grundschutz wird von den befragten Organisationen **überwiegend als umsetzbar** eingeschätzt, erfordert jedoch aufgrund seiner Komplexität einen nicht zu unterschätzenden Aufwand bei der Umsetzung (vgl. Abbildung 7). Für kantonale Stellen und kleinere (externe) Dienstleister ist die Umsetzung etwas schwieriger, weil die Vorgaben des IT-Grundschutzes sich nur schwer auf ihre Gegebenheiten anpassen lassen.

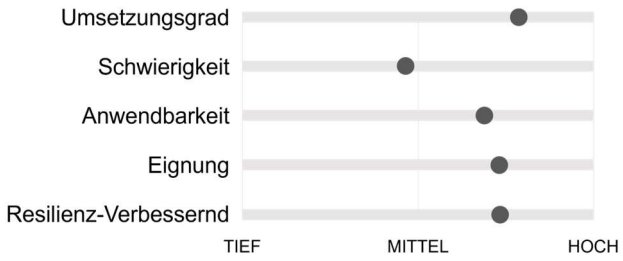

Abbildung 7: Umsetzbarkeit und Wirksamkeit der IT-Grundschutz-Vorgaben

Die **Wirksamkeit** der IT-Grundschutz-Vorgaben wird **positiv bewertet**, ist jedoch stark von den spezifischen Bedürfnissen und bereits bestehenden Sicherheitsniveaus einer Organisation abhängig. IT-Grundschutz-Vorgaben werden grösstenteils als geeignet erachtet und tragen grundsätzlich dazu bei, die Cyber-Resilienz einer Organisation zu erhöhen – insbesondere bei Organisationen, die nicht bereits ISO/IEC 27001:2022 oder ähnliche Standards implementiert haben.

Im Gegensatz zu der Umsetzbarkeit und Wirksamkeit gibt es bezüglich der **Vollständigkeit** und **Aktualität** der IT-Grundschutz-Vorgaben Vorbehalte. Die Vorgaben decken zwar eine breite Palette an Sicherheitsvorgaben ab, es scheint jedoch nicht allen Organisationen klar zu sein, welche Vorgaben sie tatsächlich umsetzen müssen. Insbesondere geht es dabei um den Geltungsbereich der neben dem IT-Grundschutz zusätzlich vorhandenen Hilfsmitteln. Das führt dazu, dass die Einhaltung des IT-Grundschutzes in der Praxis nicht vollständig ist. Das liegt unter anderem daran, dass keine klare Abgrenzung zwischen Vorgaben für Bundesstellen und Vorgaben für andere Organisationen besteht. Zudem sind neue Sicherheitskonzepte wie Cloud-Sicherheit, Zero Trust und Microsegmentation nicht hinreichend in den Vorgaben reflektiert. Die Resilienz-Wirkung könnte somit durch eine stärkere Berücksichtigung aktueller Sicherheitsentwicklungen noch erhöht werden.

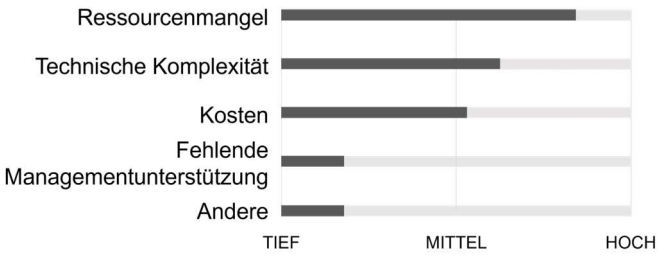

Abbildung 8: Herausforderungen bei der Umsetzung

Die Umsetzung des IT-Grundschutzes stellt insbesondere für kleinere Organisationen und Abteilungen eine **Herausforderung** dar, da es schwierig ist, ausreichend geeignetes Personal und finanzielle Mittel dafür bereitzustellen (vgl. Abbildung 8). Die technische Komplexität des IT-Grundschutzes erfordert Fachwissen und verursacht Aufwand bei der Anpassung an aktuelle Sicherheitsentwicklungen.

Die bisherige **Kommunikation** des Bundes in Bezug auf Änderungen und Anpassungen des IT-Grundschutzes wird als uneinheitlich und teilweise verbesserungsbedürftig wahrgenommen (vgl. Abbildung 9). Es fehlen regelmässige Informationsveranstaltungen und Schulungsangebote werden nicht aktiv kommuniziert, sind teilweise nicht bekannt oder nicht ausreichend praxisnah.

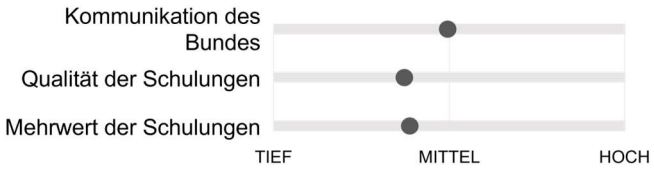

Abbildung 9: Kommunikation und Schulungen des Bundes zu den IT-Grundschutz-Vorgaben

3.2 Beurteilung der Unterschiede nach Organisationen

Die Bundesbehörden, die Kantone und die (externen) Dienstleister des Bundes beurteilen die Wirksamkeit und Umsetzbarkeit der IT-Grundschutz-Vorgaben teilweise sehr unterschiedlich.

Diese Unterschiede sind in Abbildung 10, Abbildung 11 und Abbildung 12 ersichtlich.

- Der Umsetzungsgrad der Vorgaben ist bei Kantonen tiefer als bei (externen) Dienstleistern oder Bundesstellen. Insbesondere kleinere Kantone (und kleinere Dienstleister) melden, dass es aus Ressourcengründen herausfordernd sein kann, den IT-Grundschutz umzusetzen.
- Viele Dienstleister besitzen durch die Anwendung von ISO/IEC 27001 oder von anderen Standards bereits ein gutes Sicherheitsniveau und erfüllen dadurch viele Anforderungen des IT-Grundschutzes des Bundes. Das zeigt sich in der tieferen Bewertung des Schwierigkeitsgrades und der höheren Bewertung des Umsetzungsgrades bei (externen) Dienstleistern.
- Die Interviews mit kantonalen Stellen und (externen) Dienstleister haben ergeben, dass nicht alle Hilfsmittel des Bundes allen Organisationen bekannt sind. Auch die Abgrenzung, welche Vorgaben von welchen Organisationen umzusetzen sind, gestaltet sich schwierig.
- Derzeit wird die Umsetzung des IT-Grundschutzes nicht im vollen Umfang überprüft. Es gibt keine Vorgaben dazu, was insbesondere für Organisationen mit ausgelagerten IT-Services eine Herausforderung darstellt.

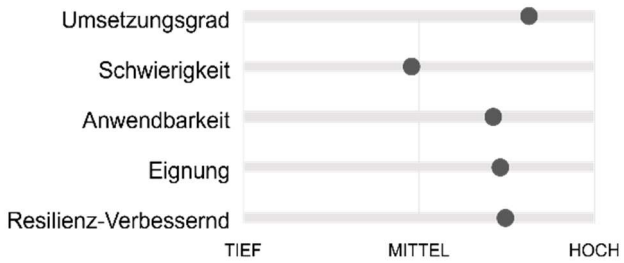

Abbildung 10: Umsetzbarkeit und Wirksamkeit des IT-Grundschutzes bei **Bundesstellen**

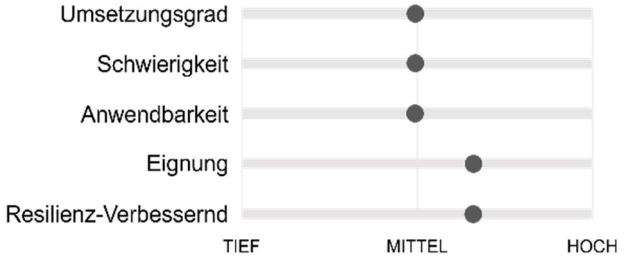

Abbildung 11: Umsetzbarkeit und Wirksamkeit des IT-Grundschutzes bei **Kantonen**

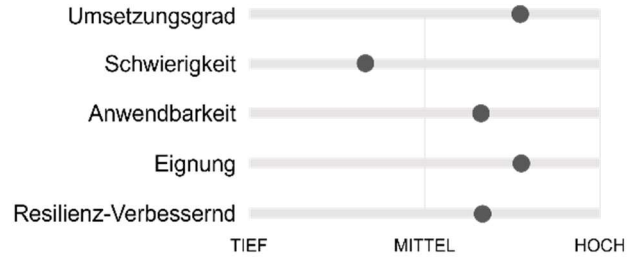

Abbildung 12: Umsetzbarkeit und Wirksamkeit des IT-Grundschutzes bei **(externen) Dienstleistern**

4 REVISIONSBEDARF, KRITIKALITÄT UND LÖSUNGSVORSCHLÄGE

Aus den oben dargelegten Erkenntnissen kann abgeleitet werden, dass der IT-Grundschutz des Bundes den grundlegenden Informationssicherheitsanforderungen durchaus Rechnung trägt. Dies ist aus den uns zur Verfügung gestellten Dokumenten und Vorgaben ersichtlich, auch wenn diese nicht in allen Aspekten den Erwartungen an ein kohärentes Rahmenwerk entsprechen. Auch die Befragten haben mehrfach betont, dass der IT-Grundschutz ein wertvolles Instrument zur Sicherstellung einer Basis-Resilienz ist. Diese Einschätzung unterstreicht die Absicht des Bundes, der Informationssicherheit mehr Raum und Gewichtung zu geben und zeigt das Potenzial, den IT-Grundschutz in eine zukunftsorientierte Richtung weiterzuentwickeln. Dabei ist zu berücksichtigen, die Basis der heute aktuellen Version des IT-Grundschutzes vor etwa 20 Jahren geschaffen und seither organisch auf aktuelle Anforderungen und Gegebenheiten angepasst wurde.

Es darf nicht ausser Acht gelassen werden, dass der IT-Grundschutz in einen übergeordneten Kontext eingebettet wird, der mittels eines umfassenden Informationssicherheits-Rahmenwerks darauf abzielt, die Informationssicherheit in der Bundesverwaltung, den Kantonen und den (externen) Dienstleistern des Bundes nachhaltig zu regeln.

Die InfoGuard AG hat aus der unabhängigen Überprüfung und Beurteilung der Bundesvorgaben zum IT-Grundschutz den folgenden Revisionsbedarf identifiziert, um einen stärker Rahmenwerk-orientierten Ansatz zu verfolgen.

Für die folgenden Liste wurden ausschliesslich die Top-2 Lösungsvorschläge der einzelnen Kategorien aufgeführt. Weitere Vorschläge finden sich im Anhang.

#	Revisionsbedarf	Lösungsvorschlag	Kritikalität
Rahmenwerk			
F.1	Ein transparenter Aufbau und eine übersichtliche Struktur der für die Informationssicherheit relevanten Elemente (Prozesse, Vorgaben, Hilfsmittel etc.) ist nicht vorhanden. Dies erschwert ein umfassendes Verständnis des IT-Grundschutzes des Bundes	Etablieren eines Informationssicherheits-Rahmenwerks, basierend auf bewährten Standards, Normen und Strukturen, nach welchem sich die Bundesbehörden, die Kantone und die externen Dienstleister des Bundes orientieren können.	Hoch
F.2	Die Abgrenzung zwischen IT-Grundschutz und der Sicherheitsstufe «hoher Schutz» ist zum Teil unklar und es sind Vorgaben oder Details in der Sicherheitsvorgabe Si001 beschrieben, welche einer höheren Sicherheitsstufe zuzuschreiben wären. Dies hat in der aktuellen Version des Dokuments auch zur Folge, dass nicht immer klar ersichtlich ist, in welchem Fall die Vorgaben anzuwenden sind.	Die Abgrenzung zwischen den Sicherheitsstufen ist klar und durchgängig aufzuzeigen. Dadurch wird auch die Klarheit bezüglich Anwendbarkeit erhöht.	Hoch
Dokumentation			
D.1	Bei «Si001 IT-Grundschutz» als «Master-Dokument» mit Grundsätzen, Prinzipen und Vorgaben sollte der Abdeckungsgrad (Scope) gegenüber ISO/IEC 27001:2022 grösser sein. Siehe auch Kapitel 2.2.	Anpassen der Sicherheitsvorgabe Si001 an die relevanten Vorgaben im ISO/IEC 27001:2022 Standard sowie an die aktuelle Risikolage und «best practices».	Hoch
D.2	Speziell in der Sicherheitsvorgabe Si001 (und auch anderen Dokumenten) ist die Grenze zur Sicherheitsstufe «hoher Schutz» teilweise unklar. Die Sicherheitsvorgabe Si001 beinhaltet auch Vorgaben, welche (nur) für höhere Sicherheitsstufen gelten. Siehe auch F.2	Anpassen der Sicherheitsvorgabe *Si001* an die Sicherheitsstufe IT-Grundschutz. Die Abgrenzung zwischen den Sicherheitsstufen muss präziser beschrieben sein.	Hoch
Kommunikation			
K.1	Für diese Beurteilung wurden keine Schulungen oder Schulungsunterlagen analysiert. Das Feedback aus der Umfrage lässt aber darauf schliessen, dass zu den Themen Kommunikation und Ausbildung ein proaktiverer Ansatz gewünscht ist.	Aufbau oder Erweiterung des Angebots für Kommunikation und Schulung für die internen und externen Stellen, welche den IT-Grundschutz umsetzen.	Mittel
K.2	Notwendige Informationen, welche die Umsetzung des Sicherheitsverfahrens unterstützen, sind schwierig zu finden (da verstreut, schwierig auffindbar oder kein Zugriff für externe Stellen).	Zentralisieren des Angebotes von Informationen und Unterlagen mittels eines «Hubs», um diese so den internen und externen Stellen zur Verfügung zu stellen.	Mittel
Prüfung			
P.1	Es fehlen konkrete Vorgaben zur Prüfung der Umsetzung und Einhaltung von Sicherheitsanforderungen sowie zur Beurteilung der Wirksamkeit der getroffenen Massnahmen.	Entsprechende Vorgaben und notwendige Verfahren zur Überprüfung von «design und operating effectiveness» sollten definiert und umgesetzt werden.	Hoch
P.2	Regelmässige Prüfungen/Audits, sowohl bei internen wie auch externen Dienstleistern, finden nicht statt respektive werden nicht vorgegeben.	Definition von Vorgaben zur regelmässigen, risikobasierten Prüfung/Auditierung von (externen) Dienstleistern	Hoch

5 FAZIT

Der IT-Grundschutz bietet eine organisch gewachsene und solide Grundlage, die unter den bisherigen regulatorischen Vorgaben eine gute Basis für die Informationssicherheit darstellt. Allerdings zeigt die Befragung der Organisationen und die unabhängige Beurteilung durch InfoGuard AG, dass in verschiedenen Bereichen Verbesserungspotenzial besteht, um die Vollständigkeit, Aktualität, Wirksamkeit und praktische Umsetzbarkeit zu erhöhen.

Ein transparenter und übersichtlicher Aufbau der sicherheitsrelevanten Elemente fehlt, was das Verständnis des IT-Grundschutzes erheblich erschwert. Insbesondere die inkonsistente Abgrenzung zwischen dem IT-Grundschutz und der Sicherheitsstufe «hoher Schutz» führt zu Unklarheiten, wodurch die Anwendbarkeit der Vorgaben nicht immer eindeutig ist. Darüber hinaus deckt die Sicherheitsvorgabe Si001 den Standard ISO/IEC 27001:2022 nicht hinreichend ab.

Wir empfehlen die Erarbeitung eines systematischen Rahmenwerks, das auf einer strukturierten Herangehensweise basiert und eine klare Einstufung der Vorgaben nach Sicherheitsstufen beinhaltet. Dieses Rahmenwerk sollte eine differenzierte und zielgerichtete Bearbeitung von Risiken und Bedrohungen ermöglichen. Die Anforderungen aus regulatorischen Vorgaben (ISG/ISV und weitere Vorgaben) sowie die relevanten Anforderungen aus ISO/IEC 27001:2022 sollten in konkrete, handlungsorientierte Massnahmen übersetzt werden, welche auf die jeweilige Schutzobjektart zugeschnitten sind. Damit wird eine gesamtheitliche Sicht auf alle relevanten Schutzobjekte und Sicherheitsmassnahmen gewährleistet. Um den gesamten PDCA-Zyklus abzudecken, sollte der IT-Grundschutz um Vorgaben und Massnahmen zur Überprüfung der Umsetzung und Wirksamkeit ergänzt werden.

Darüber hinaus sollte ein prozessbasierter Ansatz, wie er in der ISV (3. Abschnitt) skizziert ist, in einer übergeordneten «ISMS-Weisung» konkretisiert werden. Diese Weisung sollte die für ein ISMS notwendigen Prozesse – wie Risikomanagement, Ausnahmemanagement und Vorfallmanagement – sowie übergeordneten Themenbereiche integrieren und nahtlos in das gesamte Rahmenwerk eingebettet werden.

6 DANK

Wir danken dem Staatssekretariat für Sicherheitspolitik SEPOS für das mit dem Auftrag entgegengebrachte Vertrauen und allen am Projekt beteiligten Personen für die kompetente Begleitung während der Untersuchungen. Wir durften jederzeit eine sehr konstruktive und offene Zusammenarbeit mit allen beteiligten Personen geniessen.

InfoGuard AG

Annatina Vinzens
Cyber Security Consultant

Hans-Ueli Riesen
Senior Cyber Security Consultant

André Mäder
Senior Cyber Security Consultant

Levente J. Dobszay
Senior Cyber Security Consultant

Martin Rohrer
Senior Cyber Security Consultant