Hochschule Wismar
Fakultät für Ingenieurwissenschaften
Bereich Elektrotechnik und Informatik

Master-Thesis

IT-Grundschutz des BSI im internationalen Vergleich

verkürzte Fassung zur Veröffentlichung

Eingereicht am: 30. Juni 2024
von: Martin Schneider
geboren am 22.07.1969
in Hamburg

1. Prüfer: Prof. Dr.-Ing. Antje Raab-Düsterhöft
2. Prüfer: Prof. Dr.-Ing. habil. Andreas Ahrens

Aufgabenstellung

Gegenstand der Master-Thesis sind Empfehlungen, Ansätze und Vorgehensweisen, die das Ziel haben, ganzheitliche IT-Sicherheit in Organisationen zu erreichen, wobei ein besonderer Schwerpunkt auf dem IT-Grundschutz des BSI liegt.

Hierzu sind zunächst entsprechende Ansätze aus anderen Ländern zu recherchieren, vorrangig von den jeweiligen Behörden für Cybersicherheit veröffentlichtes Material. Zusätzlich sind die vielen Ansätzen zugrundeliegenden Standards ISO/IEC 27001 sowie das NIST Cybersecurity Framework und NIST SP 800-53 zu berücksichtigen.

Ausgewählte Ansätze sind mit dem IT-Grundschutz zu vergleichen. Als Fazit ist eine kritische Diskussion und Bewertung des IT-Grundschutzes im internationalen Vergleich vorzunehmen und denkbare Ansätze für eine Weiterentwicklung des IT-Grundschutzes sind aufzuzeigen.

Ferner ist der IT-Grundschutz MITRE ATT&CK und dem MITRE D3FEND gegenüberzustellen. Es ist herauszuarbeiten, inwieweit Anforderungen des IT-Grundschutzes die von MITRE ATT&CK empfohlenen Gegenmaßnahmen abdecken und gegen exemplarische in MITRE dokumentierte Angriffstechniken wirksam sind. Als Ergebnis sind wiederum eine kritische Diskussion und Bewertung des IT-Grundschutzes vorzunehmen.

Kurzreferat

Diese Arbeit betrachtet den IT-Grundschutz des BSI und die zugrundeliegende ISO/IEC 27001 sowie insgesamt 30 andere Ansätze aus 17 Ländern hinsichtlich ihrer Ziele, Vorgehensweisen und empfohlenen Sicherheitsmaßnahmen. Es zeigt sich eine Zweiteilung in sechs Ansätze für Informationssicherheit und ISMS basierend auf ISO/IEC 27001 sowie deutlich mehr für Cybersicherheit, eigenständig formuliert oder basierend auf dem amerikanischen NIST Cybersecurity Framework. Eine risikobasierte Betrachtung ist die dominierende Gemeinsamkeit. Es gibt keinen anderen Ansatz mit einer vergleichbar ausführlichen Methodik und so zahlreichen, in Bausteinen organisierten Anforderungen wie im IT-Grundschutz-Kompendium. Es ergeben sich eine Reihe von Ansatzpunkten für mögliche Verbesserungen und Weiterentwicklung des IT-Grundschutz.

Im Versuch einer Gegenüberstellung des IT-Grundschutzes mit MITRE ATT&CK und D3FENSE zeigt sich, dass ein detaillierter Vergleich mit MITRE ATT&CK im Detail sinnvolle Konkretisierungen für den Grundschutz liefern kann.

Abstract

For comparison with the German IT-Grundschutz, this thesis examines the underlying ISO/IEC 27001 and a total of 30 other approaches from 17 countries with regard to their objectives, methodologies and recommended security measures. There is a split into six approaches for information security and ISMS based on ISO/IEC 27001 on the one hand and cyber security on the other, formulated autonomously or based on the American NIST Cybersecurity Framework. A risk-based approach is the predominant common feature. There is no other approach with a comparably detailed methodology and similarly numerous requirements organized as in the IT-Grundschutz-Kompendium. A number of opportunities for possible improvements and further development of IT-Grundschutz is identified.

An attempt to compare IT-Grundschutz with MITRE ATT&CK and D3FENSE shows that MITRE ATT&CK can provide useful refinements for IT-Grundschutz.

Inhaltsverzeichnis

1 Einleitung

1.1 Motivation und Ziel der Arbeit

IT-Sicherheit ist das Thema des Studiengangs zu dieser Master-Thesis und die Frage „Wie kann man sie erreichen?“ eine Motivation für diese Arbeit. Die Frage bezieht sich auf systematische und ganzheitliche Gewährleistung von IT-Sicherheit in Organisationen beliebiger Art, was einen umfassenden Blick durch viele Einzelthemen und eine angemessene Methodik erfordert. In Deutschland ist dafür der IT-Grundschutz des BSI der maßgebliche nationale Standard und zusammen mit dem zugrundeliegenden internationalen Standard ISO/IEC 27001 dominierend. Beide haben ihre Vor- und Nachteile und Alternativen dazu scheinen dünn gesät, so dass ein Blick über die Grenzen hinaus naheliegend scheint. Zu erkunden, was sozusagen hinter dem Horizont liegt und in Ansätzen anderer Länder nach Unterschieden, Gemeinsamkeiten und sinnvollen Anregungen für Verbesserungen zu suchen, ist das Ziel, da hierzu kein befriedigendes Material aus dem Studium und eigener Berufspraxis bekannt ist.

Die Grundidee ist, einen Satz von vergleichbaren Ansätzen aus internationalen Publikationen zu finden, dahingehend zu untersuchen und in einem kritischen Vergleich dem IT-Grundschutz gegenüberzustellen.

1.2 Abgrenzung der Aufgabenstellung

Betrachtungsgegenstand sind Ansätze zur IT-Sicherheit, die einen ganzheitlichen Schutz von Unternehmen oder anderen Organisationen zum Ziel haben. Die breiter gefasste Informationssicherheit (zur begrifflichen Abgrenzung siehe Abschnitt 3.1) wie im IT-Grundschutz ist dabei willkommen, aber nicht Voraussetzung.

Die Arbeit beschränkt sich auf frei verfügbare und auf Deutsch oder Englisch veröffentlichte Ansätze. Ihr Fokus liegt auf zusammenfassender, vergleichender Betrachtung der ausgewählten Ansätze sowie einer kritischen Diskussion.

Zur Eingrenzung des Umfangs sind *nicht* Teil der Aufgabenstellung:

- Details zur Vorgehensweise der in vielen Ansätzen zentralen Risikoanalysen
- branchenspezifische Ansätze (z. B. PCI DSS, DORA, Sicherheit für industrielle Steuerungssysteme)
- Integration der IT-Sicherheit in umfassendere Management-Systeme oder Unternehmensprozesse
- Methoden zur sicheren Software-Entwicklung
- Business Continuity Management (BCM)
- für den Schutz personenbezogener Daten spezifische Aspekte
- breiter gefasste Ansätze zur Unternehmenssteuerung, in denen die IT-Sicherheit nur einen kleinen Teil ausmacht (z. B. ITIL, COBIT)

1.3 Stand der Forschung

Ein Forschungsstand für die beschriebene Aufgabenstellung ist aus einer Literaturrecherche nicht erkennbar.

Es gibt diverse Literaturhinweise zur Umsetzung von ISO/IEC 27001, die sich jedoch recht eng an den Standards orientieren und ihn Schritt für Schritt erläutern, weniger kritisch hinterfragen und noch weniger vergleichend betrachten [1] [2] [3] [4] [5, S. 107 ff.]. Von der für die ISO/IEC-Familie 27001 verantwortlichen Arbeitsgruppe gibt es unter dem Titel „The Future Landscape of ISMS Standards“ einen Ausblick, wie sich die ISO/IEC-Dokumente entwickeln sollen, aber ohne jeglichen Verweis auf andere Standards [6].

Der IT-Grundschutz selber nennt fünf weitere Standards [7, S. 13]:

- COBIT 5, ITIL und PCI DSS – diese fallen nicht in die Abgrenzung der Aufgabenstellung (siehe 1.2)
- NIST SP 800-53 – dieser Standard ist berücksichtigt (siehe 4.10)
- „Standard of Good Practice“ des Information Security Forum – dieser Standard ist nicht frei verfügbar [8]. Zudem ist er nach eigener Aussage mit ISO/IEC 27001 und NIST Cybersecurity Framework abgestimmt und verspricht daher keine zusätzlichen Erkenntnisse.

Das für die in der Beratungsbranche renommierte CISSP-Zertifizierung maßgebliche Material nennt ebenfalls nur wenige international anerkannte und hier berücksichtigte Ansätze sowie branchenspezifische, die nicht in die Aufgabenstellung fallen [9, S. 17].

Das Standardwerk von Eckert zur IT-Sicherheit beschreibt den IT-Grundschutz unter der Überschrift „Security Engineering“, also dem Entwicklungsprozess zur Konstruktion sicherer Systeme und nennt dies „eine methodisch noch nicht ausgearbeitete Disziplin“ [10, S. 171 ff.]. Unter gleichem Titel ist Anderson ein gerne zitiertes Werk [11], fokussiert aber mehr auf viele technische Grundlagen der IT-Sicherheit in Systementwicklung und -design, weniger auf ihre Umsetzung in Organisationen gemäß der Aufgabenstellung.

Eine weitere Literaturrecherche mit Kombinationen naheliegender Suchbegriffe wie „ISMS“, „Cybersecurity“, „Frameworks“, „Methodologies“, „ISO 27001 alternatives“, „IT-Grundschutz Alternativen“ etc. im Berlin-Brandenburger Bibliotheksverbund KOBV sowie bei Google Scholar brachte auch keine passenden Ergebnisse.

Zur beabsichtigten Gegenüberstellung des IT-Grundschutzes mit MITRE ATT&CK waren keinerlei Quellen zu finden.

2 Thesen

Thema: IT-Grundschutz im internationalen Vergleich

Bearbeiter: Martin Schneider

- Der IT-Grundschutz ist mit seiner umfangreichen Methodik und dem in Bausteine gegliederten Grundschutz-Kompendium einzigartig und besetzt eine offensichtliche Lücke als Umsetzungshilfe zur ISO/IEC 27001.
- Eine risikobasierte Vorgehensweise ist die große Gemeinsamkeit aller international etablierten Ansätze.
- Internationale Resonanz hat der IT-Grundschutz kaum gefunden.
- In Deutschland dominieren mit dem IT-Grundschutz und ISO/IEC 27001 Ansätze zur Informationssicherheit und einem ISMS; in anderen nationalen Ansätzen liegt der Fokus mehrheitlich auf Cybersicherheit.
- Ein etablierter, ganzheitlicher und klar auf Cybersicherheit fokussierter Ansatz fehlt in Deutschland. Eine Integration in den IT-Grundschutz wäre naheliegend, zeitgemäß sowie risikoadäquat.
- Im Detail zeigt sich erhebliches Potential für Weiterentwicklung und Verbesserung des IT-Grundschutzes. Die laufende grundlegende Überarbeitung des IT-Grundschutzes greift wichtige und sinnvolle Aspekte auf, bleibt aber – zumindest den öffentlich zugänglichen Informationen zufolge – hinter den Möglichkeiten zurück.
- Die vom IT-Grundschutz beabsichtigte Einsparung von Aufwand gegenüber ISO/IEC 27001 ist zweifelhaft.
- Die Anwendbarkeit auf kleinere Organisationen ist – auch nach Aussage des BSI selbst – nicht gegeben.
- Ein vereinfachter Einstieg für grundlegende Absicherungen wäre noch besser als bisher über Basisabsicherung und den „Weg in die Basisabsicherung“ möglich.
- Ein Abgleich mit MITRE ATT&CK würde viele sinnvolle Konkretisierungen und Ergänzungen von Grundschutz-Anforderungen liefern.

3 Grundbegriffe und Grundlagen

3.1 Informations-, IT- und Cybersicherheit

Informationssicherheit ist hier verstanden als die Bewahrung der Vertraulichkeit, Verfügbarkeit und Integrität von Informationen, in Übereinstimmung mit den Definitionen in ISO/IEC 27000 und dem IT-Grundschutz (siehe vollständige Definitionen im Anhang 8.1.1). Sie umfasst jegliche Art von Informationen, digital gespeicherte oder übertragene ebenso wie auf Papier oder nur in Köpfen von Menschen vorhandene.

Der Begriff Informationssicherheit steht üblicherweise im Zusammenhang mit einem **Informationssicherheits-Managementsystemen (ISMS)**, wie ihn der ISO/IEC-Standard 27001 geprägt hat. Es hat zum Ziel, Informationssicherheit systematisch in Organisationen umzusetzen und zu verankern.

IT-Sicherheit als die Sicherheit von datenverarbeitenden Anwendungen und Systemen deckt davon nur den Teilbereich elektronisch gespeicherter oder übertragener Information ab. Strenggenommen ist sie aber keine Teilmenge der Informationssicherheit, da sie auch den Schutz der IT-Systeme und -Anwendungen, nicht nur die in ihnen enthaltenen Informationen umfasst.

Cybersicherheit bezieht sich auf alle Risiken, die aus der Vernetzung von IT-Systemen, insbesondere dem Internet entstehen ([10, S. 41] [12], siehe auch Anhang 8.1.1). Sie ist aufgrund der historischen Entwicklung kein einheitlich definierter Begriff. Die Vorsilbe „Cyber“ taucht erstmalig 1948 in Cybernetics auf, abgeleitet aus dem Griechischen κυβερνήτης (kybernetes) = Steuermann [13]. Sie hat sich dann verselbstständigt, u. a. durch Science-Fiction-Romane, in denen 1982 erstmalig der Begriff Cyberspace auftaucht [14]. Der Begriff Cybersecurity ist lt. Oxford English Dictionary erst ab 1990 belegt [15].

Innerhalb der Cybersicherheit lassen sich Internetsicherheit und Netzwerksicherheit wie in der ISO/IEC 27032 unterscheiden [16, S. 6] und der Begriff lässt sich auch ausdehnen auf den Schutz von Menschen, Gesellschaften und ganzen Nationen vor Cyberrisiken wie in der ISO/IEC 27100 [12, S. 1].

Informationssicherheit ist der zentrale Begriff im IT-Grundschutz und dem zugrundeliegenden internationalen Standard ISO/IEC 27001, Cybersicherheit der dominierende Begriff in alternativen internationalen Veröffentlichungen und so auch den in dieser Arbeit betrachteten Ansätzen.

Zur **Häufigkeit der Begriffe** gibt es Analysen aus dem Projekt Google Books, das nach eigenen Angaben 4 % des jemals veröffentlichten Buchbestandes digitalisiert hat, überwiegend aus Universitätsbibliotheken [17]. Im englischen Sprachraum dominiert demnach inzwischen der Begriff „cybersecurity“, er hat 2016 „information security“ überholt und ist wesentlich verbreiteter als das getrennt geschriebene „cyber security“. Die leider nur bis 2019 verfügbaren Daten liefern folgendes Bild:

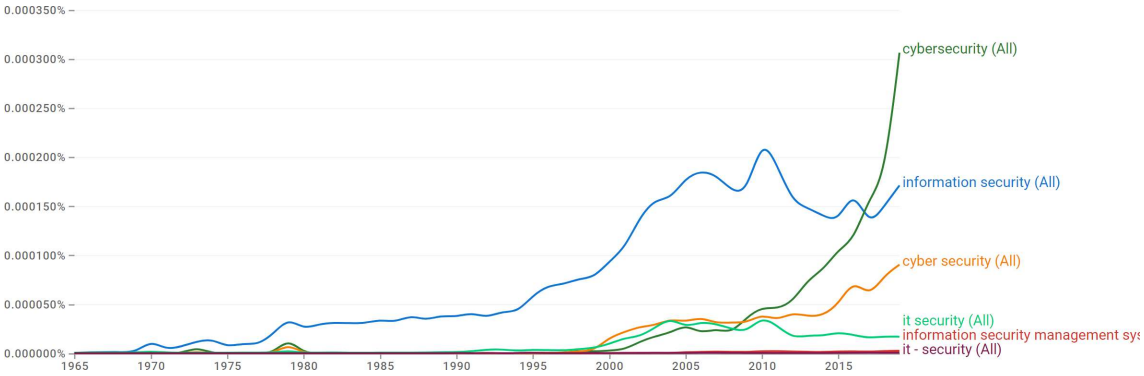


Abbildung 1: Häufigkeit der Begriffe information security, cybersecurity, cyber security u. a. im englischen Sprachraum
Quelle: [18]

Der deutsche Sprachraum weicht ab: „Informationssicherheit“ und „IT-Sicherheit“ dominieren und ein steiler Anstieg ist bis 2019 bei „Informationssicherheit“, nicht bei „Cybersicherheit“ oder „cybersecurity“ erkennbar:

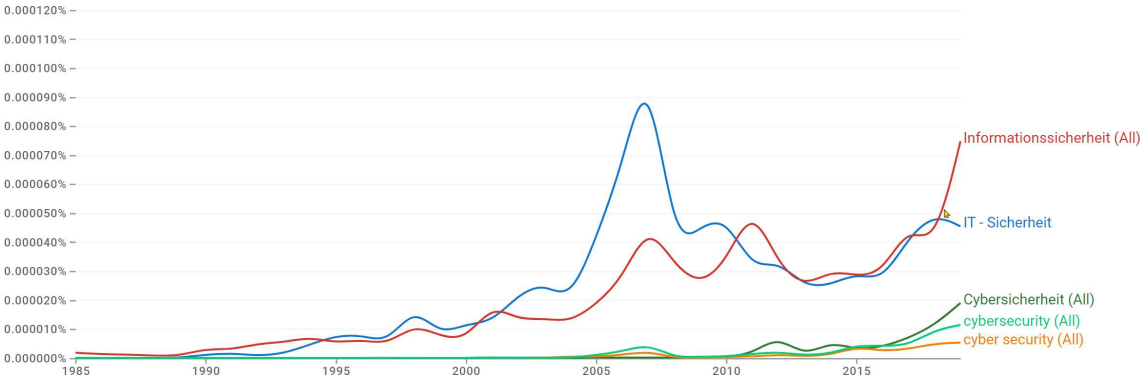


Abbildung 2: Häufigkeit der Begriffe IT-Sicherheit, Cybersicherheit, cybersecurity und cyber security im deutschen Sprachraum
Quelle: [18]

Über die Ursachen lässt sich ohne weitere Analyse, die nicht Teil der Aufgabenstellung ist, nur spekulieren. Zudem wäre eine Validierung dieser Aussage mit anderen Quellen nötig, sie ist aber stimmig mit dem Bild, das sich aus den betrachteten Ansätzen dieser Arbeit ergibt.

3.2 Sicherheitsanforderungen, -maßnahmen und „Controls“

Wesentliches Element aller ganzheitlichen Ansätze zur IT-Sicherheit ist die Auswahl von zugehörigen Maßnahmen und die Empfehlung in Form vordefinierter Kataloge. Die englischsprachigen Standards verwenden dafür den Begriff „**controls**“ und definieren ihn wie folgt:

- control = „*measure that is modifying risk*” in der ISO/IEC 27000 [19, S. 3]
- „Controls can be viewed as descriptions of the *safeguards* and protection capabilities appropriate *for achieving the particular security and privacy objectives* of the organization […]“ definiert NIST SP 800-53 [20, S. 8]

In beiden Fällen ist der Bezug zur Sicherheit wesentlicher Aspekt, einmal über die Auswirkung auf Risiken, einmal über den Zusammenhang mit Sicherheitszielen. Gleichzeitig ist es eine Abweichung von der umgangssprachlich und laut Wörterbuch naheliegenden Übersetzung „Kontrolle“, es entspricht mehr der im Englischen ebenfalls mit diesem Wort verbundenen Bedeutung „Steuerung“ oder „Lenkung“.

Der IT-Grundschutz des BSI formuliert als Entsprechung in den Bausteinen des Grundschutz-Kompendiums **Sicherheits*anforderungen*** und unterscheidet diese begrifflich von **Sicherheits*maßnahmen*** ([21, S. 7 f.], siehe auch die vollständige Definition in Anhang 8.1.2):

- Sicherheitsanforderung = „Anforderung […], deren Erfüllung zur Erhöhung der Informationssicherheit notwendig ist bzw. dazu beiträgt. […] Im englischen Sprachraum wird für Sicherheitsanforderungen häufig der Begriff ‚control‘ verwendet.“
- Sicherheitsmaßnahme = „…alle Aktionen, die dazu dienen, um Sicherheitsrisiken zu steuern und diesen entgegenzuwirken. Als englische Übersetzung wurde ‚safeguard‘, ‚security measure‘ oder ‚measure‘ gewählt“.

Er unterscheidet also zwischen Anforderungen und Maßnahmen und sieht letztere als *Aktivitäten*, die Anforderungen erfüllen. Die zugeordneten englischen Entsprechungen sind nicht ganz korrekt, wie sich aus dem Vergleich mit den direkt zuvor zitierten Definitionen aus ISO/IEC 27001 und NIST SP 800-53 erkennen lässt. NIST SP 800-53 als die umfassendste englischsprachige Sammlung von „Controls“ formuliert sie konsequent anhand von Verben – also als Aktivität.

Von praktischer Bedeutung ist diese begriffliche Unschärfe im Grundschutz-Kompendium nicht.

Diese Arbeit verzichtet auf die dort vorgenommene Unterscheidung und verwendet bevorzugt den Begriff „Sicherheitsmaßnahme“ als deutsche Entsprechung zum englischen „control“.

Im Englischen steckt die im Grundschutz beabsichtigte Unterscheidung zwischen Anforderung und Maßnahmen in der Art und Weise, wie „controls“ formuliert werden.

- NIST SP 800-53 betont, dass „controls“ ergebnisorientiert formuliert sind („outcome-based“, [20, S. xiv]).
- ISO/IEC 27001 konzentriert sich ebenfalls auf zu mit den controls zu erreichende Ergebnisse, konsequent formuliert als „… shall be …“.
- Das NIST CSF ist genauso gehalten, spricht von zu erreichenden „outcomes“ anstelle von „controls“ [22, S. i].

Dieser Aspekt der **Ergebnisorientierung** ist sehr wohl praktisch relevant, da sich das zu erreichende Ergebnis – das „was?“ – sehr generisch und allgemeingültig formulieren lässt, während der Weg dahin – das „wie?“ – je nach Kontext unterschiedlich sein kann. Dieser Aspekt taucht in der späteren vergleichenden, kritischen Betrachtung des IT-Grundschutzes wieder auf (siehe 4.3.7).

3.3 Die ISO/IEC 27000- und 27100-Familie

Die verbreiteten Normen ISO/IEC 27001 und 27002 sind Teil einer größeren Familie von Dokumenten, die einen für die Aufgabenstellung relevanten Kontext ergeben:

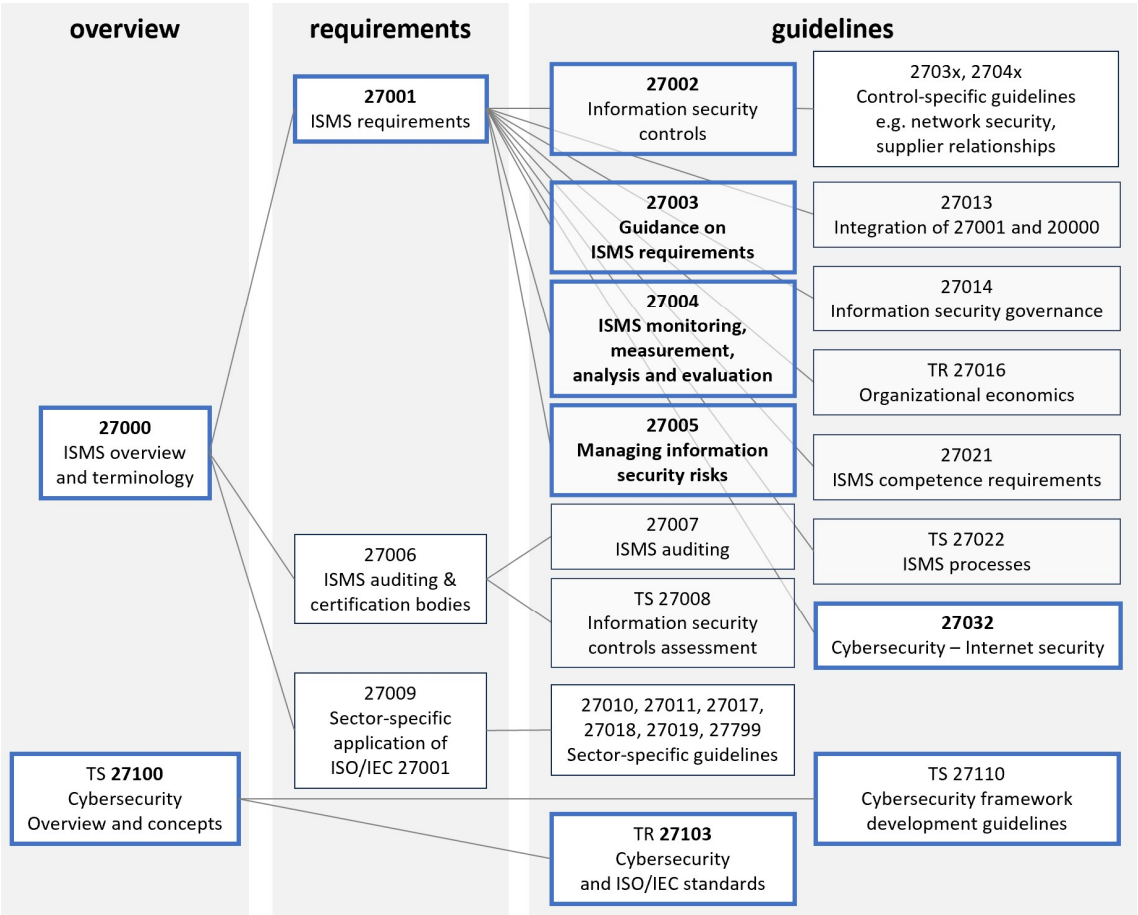


Abbildung 3: ISO/IEC 27000- und 27100-Dokumente
Quelle: Eigene Darstellung

Die drei senkrechten Bereiche veranschaulichen die Rolle der Dokumente:

- Übersichtsdokumente („**overview**“) beschreiben, wie die Dokumente einer Familie zusammenhängen und legen gemeinsame Terminologien fest.
- Anforderungen („**requirements**“) legen für eine mögliche Auditierung und Zertifizierung verbindliche Anforderungen fest.
- Empfehlungen („**guidelines**“) enthalten nicht verpflichtende Empfehlungen und Erläuterungen.

Darin sind die Dokumente mit einer reinen Zahlenangabe verabschiedete internationale Standards. „TS“ sind „technical specifications“, die zu einem

Standard vorgesehen sind, während „TR“ für „technical report“ steht und nicht verbindliche Vorgaben und ergänzende Informationen enthält [23].

Die Publikationen mit Nummerierung von 27000 – 27099 behandeln Informationssicherheit auf Basis eines ISMS mit folgender Unterteilung:

- ISO/IEC **27001** ist das Kernstück, „essence and core of the ISMS family” [6], enthält die Anforderungen an ein ISMS und sind Grundlage für eine Zertifizierung.
- ISO/IEC **27002** führt die in ISO/IEC 27001 Annex A gelisteten Controls inhaltlich weiter aus und ist damit neben ISO/IEC 27001 unverzichtbare Grundlage für ein ISMS nach ISO/IEC 27001.
- ISO/IEC **27003 – 27005** detaillieren analog andere Aspekte der ISO/IEC 27001:
  - ISMS-Anforderungen aus Kap. 4 – 10
  - Bewertung eines ISMS und
  - Vorgehen zur Risikoanalyse.
- ISO/IEC **2703x und 2704x** sind eine umfangreiche Sammlung mit weiter detaillierten Empfehlungen zu besonders wichtigen Controls der ISO/IEC 27002 und Themen wie z. B. Netzwerksicherheit, zu der als ISO/IEC 27033 alleine sieben Teile existieren.
- ISO/IEC **27032** ergänzt ISO/IEC 27002 um Aspekte der Internetsicherheit
- ISO/IEC **27006 – 27008** behandeln die Auditierung und Zertifizierung und sind für diese Arbeit nicht relevant.
- ISO/IEC **27009** und zugehörige weitere Dokumente sind branchenspezifische Ausprägungen und ebenfalls nicht relevant für die gewählte Aufgabenstellung.

Mit ISO/IEC **271xx** sind Publikationen hinzugekommen, die explizit Cybersicherheit behandeln. Letztere scheinen in der Literatur und Beratungspraxis kaum Beachtung zu finden, gemessen an den Suchergebnissen zur Literaturrecherche und Sichtung der Literatur zur ISO/IEC 27001 und 27002.

Damit ergeben sich die in der obigen Grafik mit einem blauen Rahmen hervorgehobenen ISO/IEC-Dokumente für eine genauere Betrachtung in dieser Arbeit.

3.4 Recherche ganzheitlicher Ansätze zur Informations- oder Cybersicherheit

Die Recherche nach Vergleichsmaterial zum IT-Grundschutz geschah im Internet mit zwei Blickrichtungen:

Ausgehend von den nationalen Behörden für Cybersicherheit, die über Suchmaschinen leicht auffindbar sind, lässt sich in deren Veröffentlichungen recherchieren, ob sie zu der Aufgabenstellung passendes Material veröffentlicht haben. Es zeigte sich dabei, dass „Cybersecurity“ der international dominierende Begriff ist, fast alle nationalen Behörden haben ein „Cybersecurity Centre“ oder ähnlich benannte Einrichtungen. Mitunter stehen dahinter auf operative Aufgaben und Cyberabwehr fokussierte Einrichtungen wie CERTs, die gar kein entsprechendes Material veröffentlichen.

Zum Zweiten prüfte eine Recherche nach einer Kombination aus den Schlagwörtern „Cybersecurity“ oder „information security“ plus Ländername plus „Standard“ oder „Framework“, ob auf diesem Weg weiteres Material auffindbar war.

Die Recherche umfasste folgende Länder:

- alle EU-Staaten
- alle G20-Staaten
- eine Reihe zufällig ausgewählter Länder.

Von einigen aufgrund der politischen Situation interessanten Ländern – insbesondere Russland, China, Nordkorea – war leider kein verwendbares Material zu finden, da nichts auf Englisch publiziert war oder im Falle Chinas sehr viele umfangreiche Standards veröffentlicht sind, die nur zu erheblichen Kosten beziehen sind.

Detaillierte Ergebnisse sind in Anhang 8.2, die Zusammenfassung (ohne IT-Grundschutz und ISO/IEC 27001) ist:

Beschreibung	**Anzahl Länder**	**Anzahl Ansätze**
recherchierte Länder	66	--
nur lose Veröffentlichungen zu einzelnen Themen, keine ganzheitlichen Ansätze	50	--
Sammlungen von „Best Practices“ oder einfachen, niedrigschwelligen Maßnahmensammlungen, die aber dem Anspruch genügen, einen breiten Schutz vor Cyberangriffen zu ermöglichen	8	15
umfangreiche Ansätze für ganzheitlichen Schutz in Form von vollständigen Maßnahmenkatalogen oder auch ergänzenden Vorgehensmodellen	13	16

Tabelle 1: Ergebnisse der Recherche nach ganzheitlichen Ansätzen zur IT-Sicherheit
Quelle: Eigene Darstellung

4 IT-Grundschutz und andere ganzheitliche Ansätze zur Informations- oder Cybersicherheit

4.1 Überblick betrachteter Ansätze

Das zuvor beschriebene Vorgehen ergab die folgenden in dieser Arbeit berücksichtigten Ansätze:

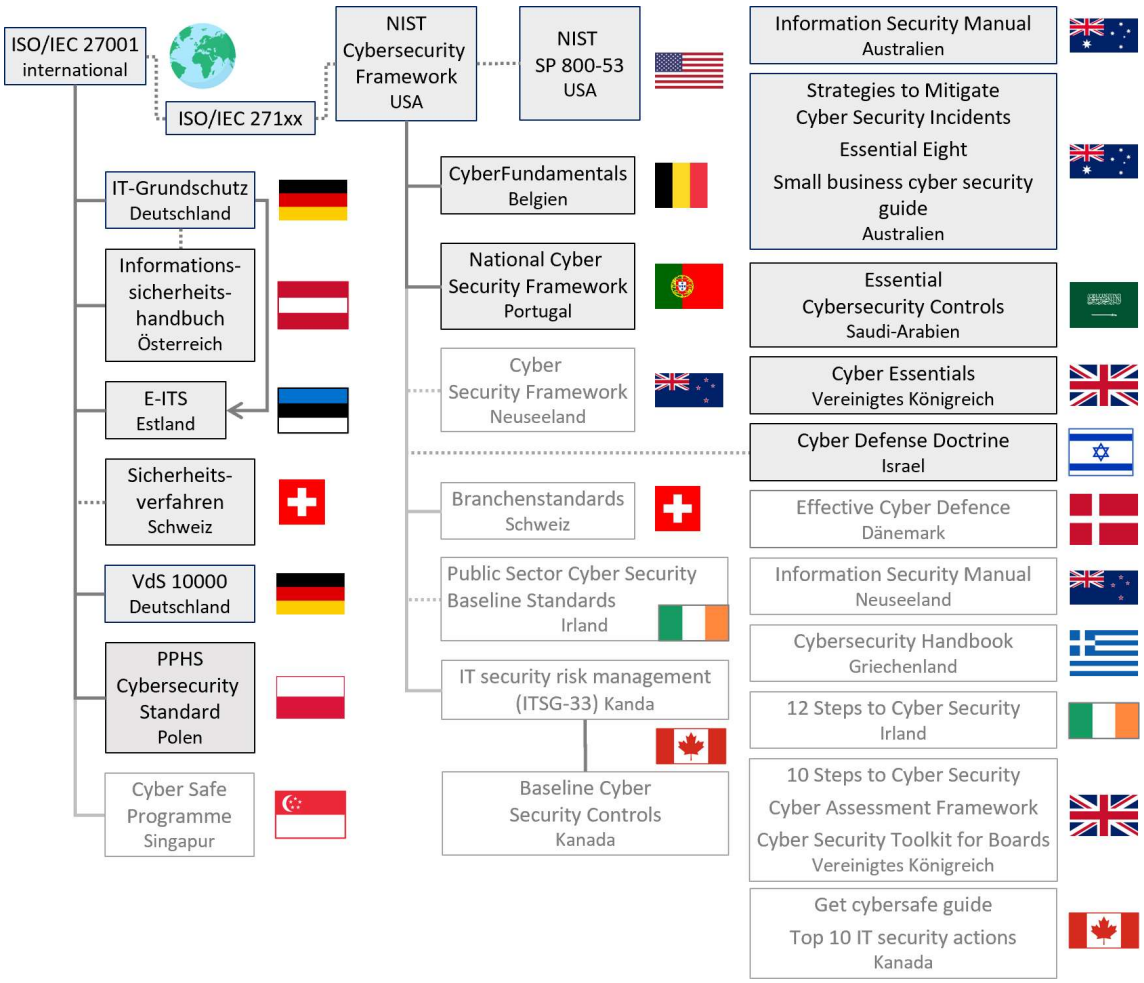


Abbildung 4: Übersicht aller betrachteten ganzheitlichen Ansätze für Informations- bzw. Cybersicherheit
Quelle: eigene Darstellung

In hervorgehobenen Kästen stehen die nach einer ersten Sichtung für am ergiebigsten befundenen und daher detailliert betrachteten Ansätze. In grauer Schrift gezeigte Ansätze sind nur mit einer kurzen Beschreibung und Bewertung berücksichtigt.

Es ergeben sich drei Säulen:

- Ganz links steht der international dominierende Standard ISO/IEC 27001 mit dem darauf aufbauenden deutschen IT-Grundschutz und anderen verwandten Ansätzen.
- In der Mitte findet sich mit dem NIST Cybersecurity Framework ein weiterer international anerkannter, in Deutschland aber wenig präsenter Ansatz mit daraus abgeleiteten Varianten.
- Ganz rechts stehen von den beiden anderen Gruppen unabhängige, eigenständige Ansätze.

Als Bindeglied zwischen ISO/IEC 27001 und dem NIST Cybersecurity Framework stehen die anscheinend wenig beachteten Veröffentlichungen der ISO/IEC 27100-Reihe, die den Zusammenhang zwischen Informations-sicherheits-Managementsystemen (ISMS) und Cybersicherheit herstellen, ihre Verbindungen miteinander und Abgrenzung voneinander aufzeigen.

4.2 ISO/IEC 27001 und 27002

4.2.1 Überblick

Ziel und Gegenstand der ISO/IEC 27001 [24] ist der Aufbau, Betrieb und die laufende Verbesserung eines vollumfänglichen ISMS zur Sicherstellung von Informationssicherheit.

Weitere Kernpunkte der Zielsetzung finden sich in der Einleitung der ISO/IEC 27001 (ebd., S. v):

- Schutz von Vertraulichkeit, Verfügbarkeit und Integrität von Information – ohne Einschränkung auf digitale Informationen oder den Bereich der Cybersicherheit
- Nutzung eines Risikomanagement-Prozesses zur Erreichung dieser Ziele
- Integration des ISMS in Unternehmensprozesse und Managementstruktur
- Anwendbarkeit auf alle Arten, Größen und Komplexitäten von Organisationen.

Die ISO/IEC 27001 ist der maßgebliche internationale Standard für ISMS, hervorgegangen aus einem bereits 1998 veröffentlichten British Standard, der diesen Begriff geprägt hat [25].

Es ist ein sehr kompaktes Schlüsseldokument mit nur 28 Seiten, das auf hoher Abstraktionsebene alle Anforderungen an ein ISMS vollständig beschreibt. Dabei sind die Inhalte der Kapitel 4 – 10, die als eigentlicher Kern der ISMS-Anforderungen gerade mal 10 Seiten ausmachen, allesamt verpflichtend für ein ISO/IEC 27001-konformes ISMS und machen keinerlei inhaltliche Vorgaben für Sicherheitsmaßnahmen.

Die Auswahl und Ausgestaltung von Sicherheitsmaßnahmen obliegen der risikobasierten Betrachtung und Entscheidung der umsetzenden Organisation. Im Anhang A der ISO/IEC 27001 aufgelistete und in der ISO/IEC 27002 [26] auf 164 Seiten erläuterte Maßnahmen haben dafür Empfehlungscharakter. ISO/IEC 27001 verlangt lediglich, die Maßnahmen aus Anhang A risikobasiert zu prüfen und einen eventuellen Ausschluss zu begründen (ebd., Kap. 6.1.3 c).

In allen Anforderungen und empfohlenen Sicherheitsmaßnahmen beschreiben die ISO/IEC-Dokumente 27001 und 27002 zu erreichende Ergebnisse und geben keine konkreten Empfehlungen zur Umsetzung – sie definieren ein „was?“ ohne Vorgaben zum „wie?“. Das lässt viel Freiraum bei der Umsetzung dieser Standards, ist ein Grund für breite Anwendbarkeit und darin begründete Akzeptanz, führt aber auch zu entsprechendem Aufwand, um die Anforderungen auf die jeweilige Organisation geeignet zu übertragen.

4.2.2 Inhaltliche Beschreibung

Relevante Dokumente

Für den Aufbau eines ISMS ist um den Standard ISO/IEC 27001 herum der in Abschnitt 3.3 erläuterte Ausschnitt der ISO/IEC 27000-Familie relevant:

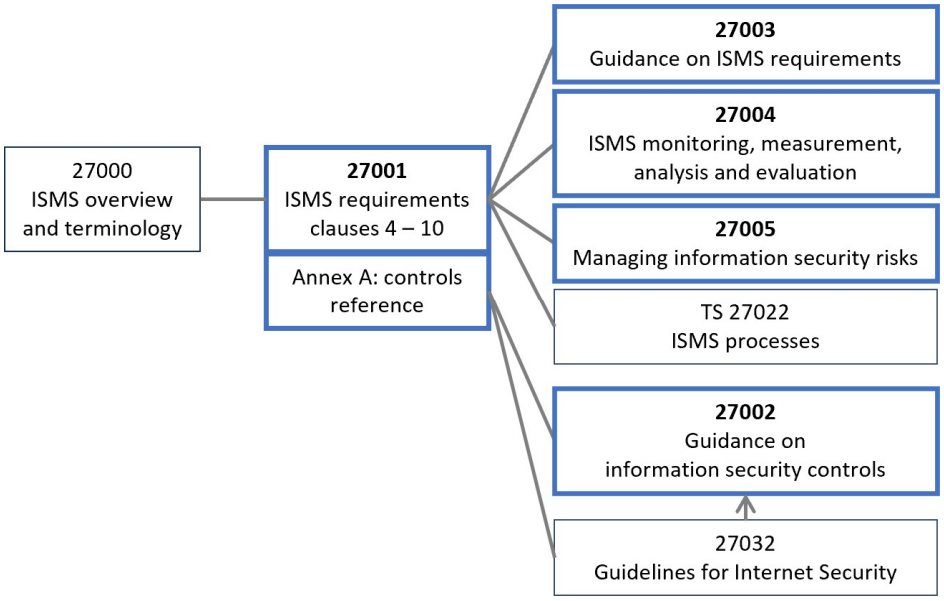


Abbildung 5: Unterstützende Dokumente zur ISO/IEC 27001
Quelle: Eigene Darstellung

Insbesondere die jüngere, erst 2021 erschienene ISO/IEC TS 27022 ist eine wichtige Hilfe bei der organisatorischen Umsetzung eines ISMS, da sie ein Prozessreferenzmodell für ein ISMS beschreibt. Die prozessorientierte Sicht erleichtert die praktische Umsetzung der maßnahmenorientierten ISO/IEC 27001-Anforderungen und deckt gleichzeitig die explizite Anforderung der ISO/IEC 27001 ab, ein ISMS zu etablieren, „… *including the processes needed* and their interactions“ (ebd. Kap. 4.4). Diese Publikation scheint in der Praxis noch keine ausreichende Beachtung zu finden; sie wird in Literatur zur Umsetzung der ISO/IEC 27001 kaum zitiert. Siehe [27] für eine ausführliche Herleitung und Validierung des Ansatzes und [28] für eine praxisnahe und anschauliche Darstellung des Prozessreferenzmodells und seiner praktischen Anwendung.

In der Praxis scheint neben der ISO/IEC 27001 vor allem die ISO/IEC 27002 genutzt zu werden, auch die zuvor genannte Literatur konzentriert sich auf diese beiden. Die gezeigten weiteren Dokumente sind aber für ein gründliches Verständnis und Anregungen zur Umsetzung genauso wichtig.

Insbesondere ist empfehlenswert,

- der ISO/IEC 27003 mit ihren Erläuterungen zu Kap. 4 – 10 das gleiche Gewicht zu geben wie der ISO/IEC 27002 und
- ISO/IEC 27032 mit ihren internetspezifischen Ergänzungen zur ISO/IEC 27002 zu berücksichtigen.

Vorgehensweise

Die ISO/IEC 27001 versteht sich ausdrücklich nicht als Vorgehensmodell, sondern ausschließlich als Sammlung von Anforderungen ohne Angabe von Prioritäten oder empfohlene Reihenfolge der Umsetzung [24, S. v].

Eine recht grobe Empfehlung zur Vorgehensweise findet sich jedoch in ISO/IEC 27000 [19, S. 14]:

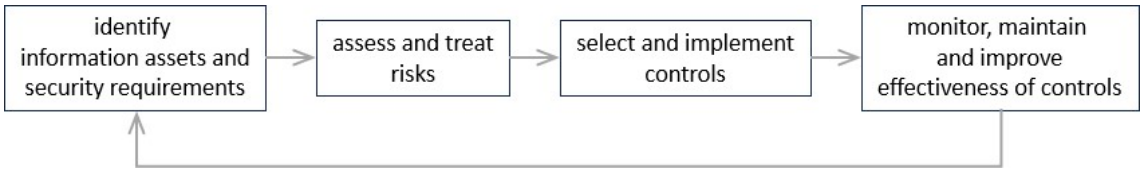


Abbildung 6: Schritte zum Aufbau und Betrieb eines ISMS
Quelle: Eigene Darstellung basierend auf ISO/IEC 27000 Kap. 4.5.1

Sie fokussiert auf die für wirksame Informationssicherheit relevanten Maßnahmen („controls“) und übergeht dabei eine Reihe von Aspekten der ISO/IEC 27001, die ein ISMS ausmachen.

Eine damit kompatible, aber wesentlich detailliertere Vorgehensweise ergibt sich aus dem logischen Zusammenhang der einzelnen Kapitel der ISO/IEC 27001:

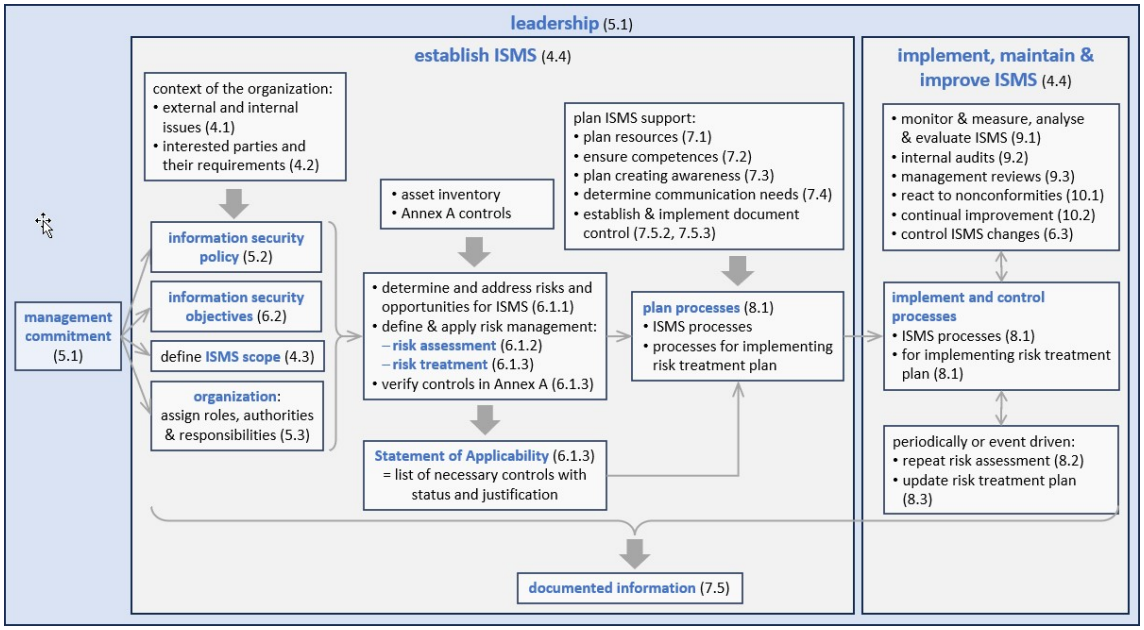


Abbildung 7: Anordnung von ISO/IEC 27001-Kapiteln zu Vorgehensmodell
Quelle: Eigene Darstellung

Die Elemente dieser Darstellung sind:

- Die **Unterstützung der Leitungsebene** ist Grundvoraussetzung für wirksame Umsetzung von Informationssicherheit, entsprechend ist „management commitment“ als Startereignis gezeigt und die weiteren Aspekte der Management-Unterstützung („leadership“) bilden einen alles umfassenden Rahmen.
- Der erste innere Kasten „**establish ISMS**“ zeigt die Aktivitäten für den anfänglichen Aufbau eines ISMS, gemäß der genauen Bedeutung von „establish“ d. h. etwas Neues einzurichten oder zu erschaffen[1].
    - Die erste Säule in diesem Kasten schafft alle für das ISMS erforderlichen **Rahmenbedingungen**: Analyse des Umfelds, Formulierung von Informationssicherheitszielen und einer Sicherheitsleitlinie, Festlegung des Geltungsbereichs, Schaffung organisatorischer Voraussetzungen.

[1] “establish something: to start or create an organization, a system, etc. that is meant to last for a long time”, siehe https://www.oxfordlearnersdictionaries.com/definition/english/establish?q=establish: abgerufen am 23.05.2024

  - Die zweite Säule beschreibt die **risikobasierte Auswahl von Sicherheitsmaßnahmen**: Anhand eines Inventars aller zu schützenden Werte („assets“) sind Risiken zu definieren und zu bewerten und erforderliche Maßnahmen für die Risikobehandlung zu identifizieren.
    Die vorgegebene Liste von Maßnahmen im Anhang A der ISO/IEC 27001 ist ein dabei zu berücksichtigender Katalog möglicher Maßnahmen.
    Als zentrales Ergebnis listet das resultierende „Statement of Applicability“ alle erforderlichen Sicherheitsmaßnahmen auf.
    Daneben sind Chancen und Risiken für das ISMS selber zu betrachten.
  - Die dritte Säule beinhaltet die **Umsetzungsplanung**, sowohl für ISMS-Prozesse als auch alle eigentlichen Sicherheitsmaßnahmen. Dazu fließen mehrere Anforderungen als notwendige Unterstützung ein wie z. B. die Bereitstellung erforderlicher Ressourcen, Qualifizierung beteiligter Mitarbeiter.
- Der rechte innere Kasten stellt nach den einmaligen bzw. erstmaligen Aktivitäten den laufenden **Betrieb des ISMS** mit Umsetzung aller Sicherheitsmaßnahmen und kontinuierlicher Verbesserung dar. Er beinhaltet auch den in der ISO/IEC 27001 geforderten Schritt der „implementation“[2], der hier begrifflich sauber vom vorgelagerten „establish“ getrennt werden soll:
  - Die Umsetzung und Aufrechterhaltung der Prozesse und der eigentlichen Sicherheitsmaßnahmen stehen im Mittelpunkt.
  - Diverse Aktivitäten zur Überwachung und Steuerung wie interne Audits, Management-Reviews tragen zur Aufrechterhaltung und kontinuierlichen Verbesserung bei.
  - Die periodische oder anlassbezogene Wiederholung der Risikobetrachtung aktualisiert von Zeit zu Zeit die definierten Sicherheitsmaßnahmen.

[2] implement = durchsetzen, “put into practice”
implement something: to make something that has been officially decided start to happen or be used”, siehe
https://www.oxfordlearnersdictionaries.com/definition/english/implement_1?q=implement,
abgerufen am 23.05.2024

- Die in der ISO/IEC 27001 nicht genau spezifizierte **Dokumentation** umfasst alle genannten Aktivitäten und daraus resultierenden Ergebnisse, die angemessener Anzahl und Strukturierung von Dokumenten sowie ihr Umfang sind von der jeweiligen Organisation selbst festzulegen.

Sicherheitsmaßnahmen

Die in der ISO/IEC 27001 empfohlenen und mindestens zu berücksichtigenden Sicherheitsmaßnahmen umfassen 93 als „controls“ bezeichnete Anforderungen, die seit der Aktualisierung in 2022 eine einfache Gliederung in vier Bereiche („Themes“) haben:

- 37 Organisatorische Maßnahmen
- 8 Personal
- 14 Maßnahmen zur physischen Sicherheit
- 34 Technische Maßnahmen.

Sie bewegen sich alle auf sehr hohem Abstraktionsniveau und erfordern für ihre praktische Umsetzung eine Reihe von detaillierteren Planungsaktivitäten und Einzelmaßnahmen.

Dabei ist ein “Control” definiert als „measure that is modifying risk“ ([19, S. 3], s. auch 3.2), also eine Maßnahme, die sich auf das Risiko für Vertraulichkeit, Verfügbarkeit, Integrität von Informationen auswirkt – entsprechend der zugrundeliegenden risikoorientierten Betrachtungsweise.

Eine genauere Analyse der einzelnen Maßnahmen ist hier nicht sinnvoll, es gibt keinen Grund, die Vollständigkeit und Angemessenheit der Maßnahmen der ISO/IEC 27001 kritisch zu hinterfragen, da die ISO/IEC 27001 ein seit Jahren bewährter, international akzeptierter und auf diese Weise vielfach praxiserprobter Standard ist.

„Themes“ und „attributes”

Die oben gezeigte Gliederung der Controls in vier Bereiche ist eine einfache Kategorisierung, die die ISO/IEC 27002 als „theme“ bezeichnet. Daneben gibt es mit der 2022 aktualisierten Fassung ein neues Konzept von „attributes“, das

beliebige andere Kategorisierungen erlaubt. Einige sind schon vorgegeben, z. B. die Zuordnung von Controls zu den Sicherheitszielen Vertraulichkeit, Verfügbarkeit, Integrität.

Zweck dieser Attribute ist, die Controls in beliebigen anderen Sichten zu filtern und zu gruppieren. Wenn sinnvoll, ist die Definition und Zuordnung beliebiger weiterer Attribute vorgesehen, um z. B. die Art der betroffenen Assets anzuzeigen.

Dokumentation

Bezüglich erforderlicher Dokumentation stellen ISO/IEC 27001 und 27002 wenige generische Anforderungen und überlassen Umfang und Gliederung der Ausgestaltung der jeweiligen Organisationen.

Eine Liste der genauen Dokumentationsanforderungen ist im Anhang 8.3, zusammengefasst ergeben sich die folgenden inhaltlichen Anforderungen:

- Grundlagendokumente zum ISMS: Leitlinie, Sicherheitsziele, Geltungsbereich
- Risikomanagement:
  - Prozess zur Risikobewertung und -behandlung
  - Ergebnisse der Risikoanalyse
- „Statement of Applicability“ als zentrale Referenz der anzuwendenden Sicherheitsmaßnahmen
- sehr generische Anforderungen im Ermessen der jeweiligen Organisation:
  - Richtlinien und andere Dokumente „as determined […] as being necessary for the effectiveness of the ISMS“
  - Arbeitsabläufe („operating procedures“)
  - Nachweisdokumente „to the extent necessary to have confidence … that the processes have been carried out”
- 17 nicht verbindliche Empfehlungen für Richtlinien zu bestimmten Themen aus der ISO/IEC 27002 (siehe ebenfalls Anhang 8.3).

4.2.3 Zusammenfassende Bewertung

Der ISO/IEC 27001-Standard ist das international maßgebliche, etablierte und untrennbar mit dem Begriff Informationssicherheit verbundene Dokument für die Definition und den Aufbau eines ISMS. Er ist für sich alleine betrachtet kompakt und überschaubar, aber mit all seinen Implikationen in der praktischen Umsetzung sowie zusammen mit den ergänzenden Standards anspruchsvoll und aufwändig in der praktischen Umsetzung.

Der Anspruch, einen für Organisationen aller Art und Größe anwendbaren Ansatz zu schaffen, bringt einen hohen Abstraktionsgrad und entsprechenden Arbeitsaufwand für die konkrete Anwendung auf einzelne Organisationen mit ihren spezifischen Anforderungen mit sich. Insbesondere ist die Erarbeitung entsprechender Vorgabedokumente in Form von zahlreichen Richtlinien aufwändig und ohne klare Vorgabe. Der Flexibilität und beliebigen Anpassbarkeit steht der hohe Aufwand als Nachteil gegenüber und schafft einen offensichtlichen Bedarf an Umsetzungshilfen.

Die recht allgemein formulierten, aber sehr breit gefassten „Controls“ im Anhang A der ISO/IEC 27001 zusammen mit ISO/IEC 27002 sind eine wichtige Referenz für einen Katalog möglicher Sicherheitsmaßnahmen.

4.3 IT-Grundschutz des BSI

4.3.1 Überblick

Als **Ziele** definiert der IT-Grundschutz in seinen Standards 200-1 [7] und 200-2 [29] sowie dem IT-Grundschutz-Kompendium [21]:

- angemessener Schutz aller Informationen einer Institution
- Aufbau eines Informationssicherheits-Managementsystems mit systematischem Vorgehen und ganzheitlichem Ansatz
- Aufwand im Informationssicherheitsprozess reduzieren.

Der IT-Grundschutz ist ein nationaler deutscher Standard und versteht sich als Umsetzungshilfe zur ISO/IEC 27001. Er ist sehr umfangreich, bestehend aus

- knapp 300 Seiten der drei BSI-Standards zu
    - ISMS (200-1, 48 Seiten),
    - Grundschutz-Methodik (200-2, 180 Seiten) und
    - Risikoanalyse (200-3, 54 Seiten)
- IT-Grundschutz-Kompendium (858 Seiten in der Edition 2023).

Besonderheiten, die er dem ISO/IEC 27001-Standard hinzufügt, sind:

- Die in den erwähnten BSI-Standards beschriebene eigene Methodik
- Die Baustein-Struktur des Kompendiums, die für verschiedene Anwendungsbereiche zahlreiche standardisierte Sicherheitsmaßnahmen vorgibt
- Die sogenannte „implizite Risikoanalyse“, d. h. eine standardisierte Risikoanalyse, die den Grundschutz-Anforderungen im Kompendium zugrunde liegt – mit der Folge, dass für sog. „normalen Schutzbedarf“ eine eigene Risikoanalyse entfällt.

4.3.2 Geschichte und Positionierung

Das BSI hat erstmalig 1994 Sicherheitsempfehlungen unter der Bezeichnung „IT-Grundschutz“ veröffentlicht [30]; diese gingen hervor aus seit 1989 veröffentlichten Empfehlungen für sichere IT.

2006 erfolgte eine Überarbeitung zur Integration des ISMS-Ansatzes aus der erstmalig 2005 veröffentlichten ISO/IEC 27001 [31], die wiederum auf einen britischen Standard aus den 1990er Jahren zurückgeht [25]. Damit erschienen die ersten BSI-Standards 100-x und zugehörigen Grundschutz-Kataloge [32] als Vorläufer des heutigen Kompendiums. Die Grundschutz-Kataloge waren sehr umfangreiche Sammlungen von Gefährdungen, Maßnahmen und Bausteinen. Die Bausteine bestanden anders als heute aus reinen Verweisen auf relevante Gefährdungen und zugehörige Maßnahmen für bestimmte Zielobjekte. Die zugehörigen Listen von Gefährdungen und Maßnahmen waren extrem lang – die Kataloge enthielten jeweils viele Hundert und hatten in der letzten Ausgabe 2016 einen Umfang von über 5.000 Seiten.

2017 erfolgte dann eine Aktualisierung zu den heute noch gültigen Standards 200-x und dem Grundschutz-Kompendium anstelle der Grundschutz-Kataloge.

Bereits der Standard 100-2 von 2008 wendete sich an „Institutionen aller Größen und Arten“ und schloss explizit Unternehmen, Behörden und sonstige öffentliche oder private Organisationen ein [32, S. 7]. Trotzdem ist eine gewisse Ausrichtung auf Behörden in Begriffen und Anforderungen erkennbar (siehe hierzu auch die kritische Diskussion in 4.3.7).

Hinzu kommt, dass der IT-Grundschutz für Behörden eine besondere Bedeutung hat. Mit dem sog. „Umsetzungsplan Bund 2017“, der Leitlinie für Informationssicherheit in der Bundesverwaltung [33] werden BSI-Standards als verbindlich für die Bundesverwaltung festgeschrieben.

Vor diesem Hintergrund ist davon auszugehen, dass die Vorgabe zahlreicher Anforderungen auf Basis einer standardisierten Risikoanalyse auch dem Ziel dient, eine Vergleichbarkeit und ein gewisses einheitliches Mindestniveau an Informationssicherheit zu forcieren.

Der IT-Grundschutz steht unabhängig neben anderen Aktivitäten des BSI zur Cybersicherheit (siehe hierzu auch Abschnitt 4.12).

4.3.3 Vorgehensweise

Die Vorgehensweise des IT-Grundschutzes ist komplex und ergibt sich zunächst aus dem Zusammenwirken der Standards 200-1 ISMS und 200-2 Grundschutz-Methodik. Der Standard 200-1 versteht sich als allgemeine Beschreibung eines ISMS, kompatibel mit ISO/IEC 27001 und unabhängig von der gewählten Methodik. Der Standard 200-2 beschreibt dann die spezielle IT-Grundschutz-Methodik [7, S. 12].

Die Hauptelemente der beiden Standards sind folgende:

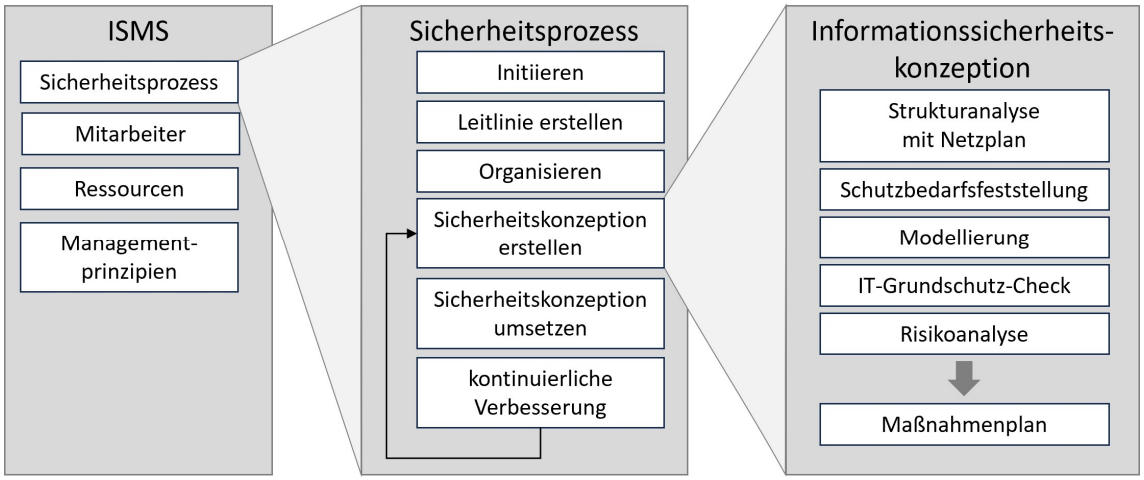


Abbildung 8: Hauptelemente der IT-Grundschutz-Methodik
Quelle: Eigene Darstellung, basierend auf BSI-Standards 200-1 S. 15 und 200-2 S. 15, 76

- Das **ISMS** selbst mit den hier gezeigten vier Bestandteilen [7, S. 15]
- der **Sicherheitsprozess**, der zunächst Sicherheitsziele und -strategie vorgibt sowie Rahmenbedingungen schafft und dann den eigentlichen Kern – das Ableiten von Sicherheitsmaßnahmen – mit seinen begleitenden Aktivitäten angeht [29, S. 15]
- die **Informationssicherheitskonzeption**, die aus den Grundschutz-Bausteinen umzusetzende Maßnahmen ermittelt, ggf. eine Risikoanalyse ergänzt und daraus einen Maßnahmenplan entwickelt [29, S. 76].
  Die Schritte der Informationssicherheitskonzeption variieren je nach Vorgehensweise, dazu mehr weiter unten.

Dabei weisen die Beschreibungen in den BSI-Standards 200-1 und 200-2 einige begriffliche Unschärfen, Unstimmigkeiten und Überschneidungen auf. Einzelne davon sind in Anhang 8.1 erklärt und belegt und hier nur im Ergebnis genannt:

- Die Rolle der Sicherheitsstrategie als Teil des ISMS ist nicht konsistent beschrieben.
- Die BSI-Standards 200-1 und 200-2 verwenden die zentralen Begriffe Sicherheits*konzept* und Sicherheits*konzeption*, ohne sie zu definieren und klar gegeneinander abzugrenzen. Das Grundschutz-Kompendium enthält Definitionen, die Verwendung der Begriffe ist aber nicht über alle drei Dokumente hinweg konsistent und kann beim Bestreben, die Methodik gründlich zu verstehen, durchaus Verwirrung entstehen lassen.

- Der „Sicherheitsprozess“ ist im Standard 200-1 nicht klar mit seinen Prozessschritten definiert und ohne leicht ersichtliche Begründung abweichend vom Standard 200-2.

Die Erstellung einer Sicherheitskonzeption, die zum Ziel hat, nach der Grundschutz-Methodik einen Satz an Sicherheitsmaßnahmen zu entwickeln und umzusetzen, ist im Standard 200-2 beschrieben und kann nach drei Vorgehensweisen erfolgen. Die zugehörigen Diagramme aus dem BSI-Standard 200-2 sind im Anhang 0 gezeigt, nachfolgend eine konsolidierte Übersicht:

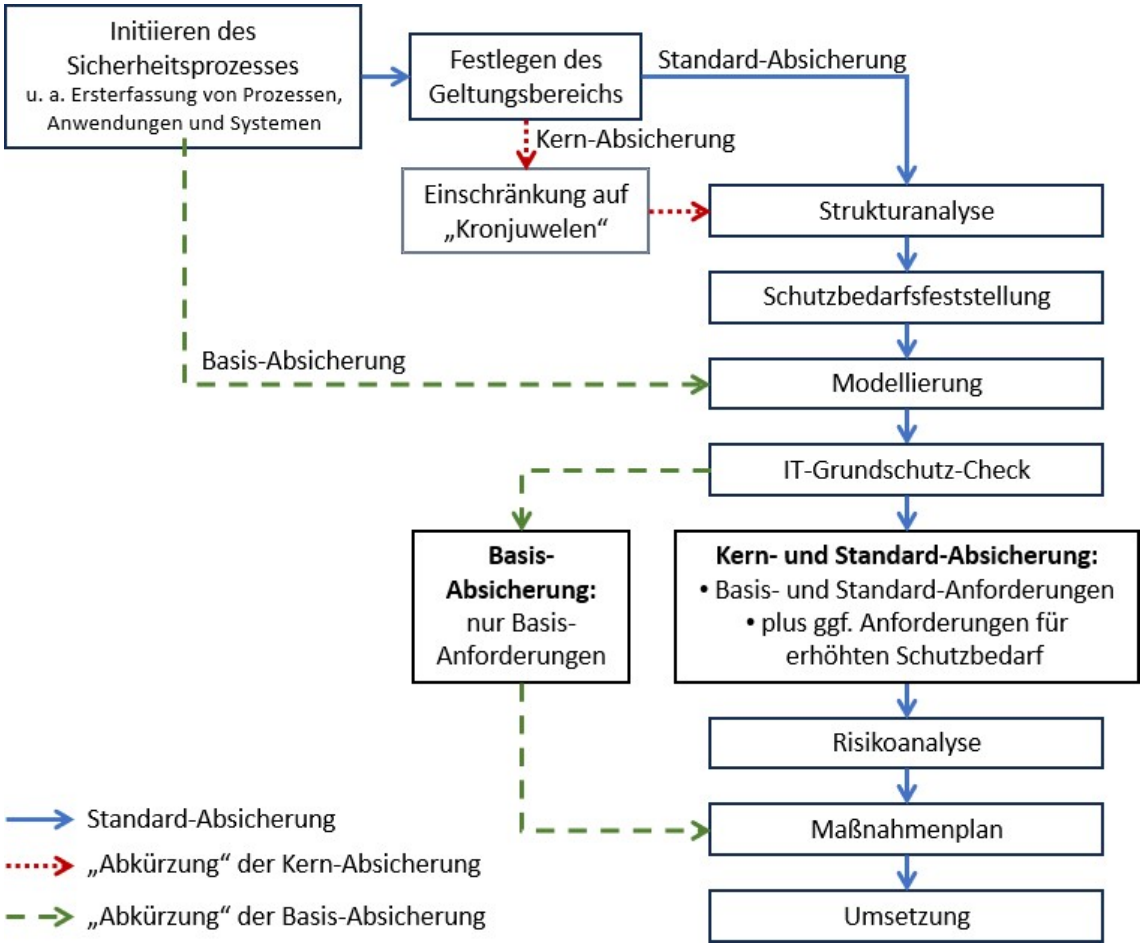


Abbildung 9: Vorgehensweisen der IT-Grundschutz-Methodik im Vergleich
Quelle: Eigene Darstellung

- **Standard-Absicherung:** Das empfohlene Standardvorgehen für einen angemessenen Schutz des gesamten Informationsverbundes, diese Vorgehensweise durchläuft alle Schritte der IT-Grundschutz-Methodik.
- **Kern-Absicherung:** Dies ist eine Reduzierung des *Geltungsbereiches* und als Folge eine beschleunigte Absicherung nur der wichtigsten Ressourcen mit einem angemessenen Schutzniveau. Entsprechend hat sie einen

zusätzlichen Prozessschritt, um die der Organisation wichtigsten und als „Kronjuwelen“ bezeichneten Ressourcen zu identifizieren. Auf diese wird der zuvor definierte Geltungsbereich reduziert und alle weiteren Schritte lassen sich anschließend mit reduziertem Aufwand durchlaufen.

- **Basis-Absicherung:** Dies ist eine Reduzierung der *umzusetzenden Maßnahmen* und als Folge eine beschleunigte Absicherung des gesamten Informationsverbundes mit einem grundlegenden Sicherheitsniveau. Entsprechend braucht sie keine Schutzbedarfsfeststellung, da für alle Ressourcen gleichermaßen ein einheitliches Basis-Sicherheitsniveau umzusetzen ist. Danach fallen auch die Grundschutz-Checks kürzer aus, da sie nur den kleineren Satz an Basis-Anforderungen berücksichtigen und keine mögliche separate Risikoanalyse durchzuführen ist.

Als weitere Verkürzung bietet das BSI den „Weg in die Basis-Absicherung“ (WiBA) an [34]. Diese richtet sich an Kommunalverwaltungen, zum Einstieg in das Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“.

4.3.4 Sicherheitsmaßnahmen

Umfang und Strukturierung

In den Sicherheitsmaßnahmen unterscheidet sich der IT-Grundschutz ebenso deutlich von dem ISO/IEC 27001-Standard wie bei der Vorgehensweise. Unter Wahrung der Kompatibilität zueinander ist der Umfang im IT-Grundschutz um ein Vielfaches gewachsen, um konkretere Vorgaben für die Ausformulierung von Sicherheitsmaßnahmen zu geben. Zusätzlich sind alle Maßnahmen im Grundschutz-Kompendium in Form von Bausteinen nach ihrem Anwendungsbereich organisiert, was das Auswählen relevanter Anforderungen erleichtert:

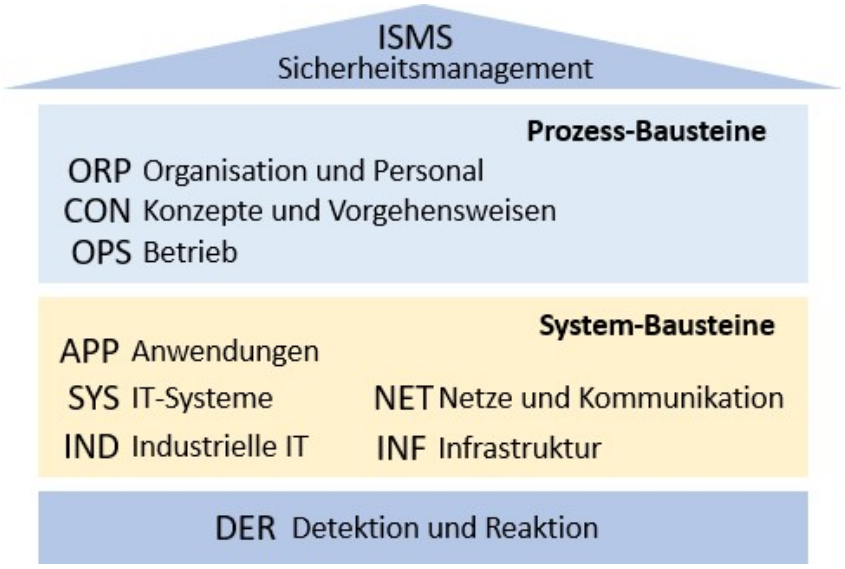


Abbildung 10: Baustein-Struktur des IT-Grundschutz-Kompendiums
Quelle: Eigene Darstellung, angelehnt an [21, Schichtenmodell und Modellierung, S. 1]

System-Bausteine sind nur auf die jeweiligen Arten von sog. „Schutzobjekten" wie Clients, Server, Netze oder auch spezielle Objekttypen wie Webbrowser, Windows-Clients etc. anwendbar.

Prozess-Bausteine betreffen den gesamten Informationsverbund oder zumindest große Teile davon. Das gilt auch für die separat gezeigten Bausteine ISMS und DER, diese stehen jedoch in eigenen Bereichen, da sie Sonderrollen haben. Der Baustein ISMS ist Grundlage für alle weiteren Aktivitäten im Sicherheitsprozess, Bausteine im Abschnitt Detektion und Reaktion überprüfen umgesetzte Sicherheitsmaßnahmen oder sind für die Detektion von und Reaktion auf Sicherheitsvorfälle entwickelt.

Der Umfang der Sicherheitsmaßnahmen ist sehr hoch:

- 111 Bausteine
- 1.835 Anforderungen, die in der Regel aus einem Absatz Fließtext bestehen, was weitere Teilanforderungen ergibt
- ca. 6.500 Teilanforderungen, die durch Aufspalten der Anforderungen in einzelne Sätze entstehen. Dies ist oft notwendig, da nebeneinanderstehende Sätze innerhalb einer Anforderung durchaus unterschiedliche Aspekte behandeln können, die separate Aktivitäten für Umsetzung und Überprüfung erfordern.

Vollständigkeit

Die sehr umfangreiche Sammlung von Sicherheitsmaßnahmen und Einbettung in ein sehr formalisiertes Vorgehen können eine Vollständigkeit und Zuverlässigkeit suggerieren, die tatsächlich nicht gegeben ist.

Die Sicherheitsmaßnahmen „bilden den Stand der Technik ab“, zeigen „was zum jeweiligen Zeitpunkt einerseits technisch fortschrittlich ist und sich andererseits in der Praxis als geeignet erwiesen hat“ [35, S. 1 im Abschnitt IT-Grundschutz – Basis für Informationssicherheit]. Es dauert naturgemäß eine gewisse Zeit, bis sich ein „Stand der Technik“ herausbildet und bewährt, von daher kann er aktuelle Entwicklungen nicht berücksichtigen. Hinzu kommt ein nur jährlicher Aktualisierungsrhythmus, der ab 2024 wegen grundlegender Überarbeitungen des Grundschutzes ausgesetzt ist. Schon diese Überlegungen verdeutlichen, dass Entwicklungen mindestens aus den letzten zwei Jahren nicht berücksichtigt sein können und alle Maßnahmen auf mögliche Aktualisierungen zu prüfen sind.

Daneben weist das BSI selbst darauf hin, dass bei hohem Schutzbedarf und bei anderen Einsatzzwecken als in den jeweiligen Bausteinen angegeben immer zusätzliche Maßnahmen, individuell anhand einer eigenen Risikoanalyse definiert, zu erwägen sind.

Prioritäten

Die Anforderungen des IT-Grundschutzes enthalten auf zwei Weisen simple Formen der Prioritätensetzung:

- Für Zielobjekte mit normalem Schutzbedarf gibt eine Abstufung in Basis- und Standardanforderungen gibt innerhalb der Anforderungen Prioritäten an.
    - Basis-Anforderungen sind vorrangig umzusetzen, da sie tendenziell mit geringem Aufwand größtmöglichen Nutzen erzielen. Sie sind fast ausnahmslos als „Muss-Anforderungen“ formuliert, was gemäß der BSI-Methodik nicht zulässt, sie als entbehrlich einzustufen und abzuwählen.
    - Standard-Anforderungen sind für eine angemessene Absicherung nach Einschätzung des BSI ebenfalls erforderlich, aber nicht ganz so vordringlich. Daneben sind sie bis auf wenige Ausnahmen „Soll-

Anforderungen“, was in der Grundschutz-Methodik bedeutet, dass sie mit entsprechender Begründung auch als entbehrlich eingestuft und übergangen werden können.

- Nur für erhöhten Schutzbedarf sind in der dritten Stufe von Anforderungen Vorschläge für zusätzliche Absicherung zu prüfen und zu ergänzen.

4.3.5 Dokumentation

Die Anforderungen an Dokumentation sind ungleich höher als in ISO/IEC 27001 und 27002, in den zahlreichen Anforderungen des IT-Grundschutzes sind viele Angaben über zu erstellende

- Richtlinien, Konzepte u. ä.
- Dokumentation von Entscheidungen, Tätigkeiten, Prüfungen etc.

Der BSI-Standard 200-2 definiert in Kap. 5 allgemeine Anforderungen an Dokumentation, gibt jedoch keine Empfehlung in Form einer beispielhaften Dokumentenstruktur und keine Abgrenzung verschiedener Arten von Dokumenten wie Richtlinien, Konzept etc., die das Grundschutz-Kompendium verwendet. Ebenso fehlen klare Anforderungen an die Dokumentenlenkung, dort und im zugehörigen Baustein ISMS.1.

Eine genaue Auswertung des Aufwandes für **Vorgabedokumente** im IT-Grundschutz ist aufwändig, da keine zentrale Übersicht existiert und die zu erstellenden Dokumente im Fließtext des Grundschutz-Kompendiums ohne besondere Hervorhebung enthalten sind. Die Anforderungen des Grundschutz-Kompendiums in Form einer XML-Datei lassen sich aber teilweise automatisiert auswerten; ein Filtern nach Begriffen wie „Richtlinie“ und „Konzept“ liefert fast 600 Fundstellen, davon knapp 400, die auf eine tatsächlich zu erstellende Dokumentation Bezug nehmen. Eine Bereinigung um Duplikate ergibt

- 54 Richtlinien
- 76 Konzepte
- 13 weitere Dokumente wie Planungen oder Spezifikationen,

die bei genauer Befolgung des IT-Grundschutzes und aus allen Bausteinen zu erstellen wären. Die gesamte Liste ist im Anhang 0. und noch nicht vollständig,

da einzelne weitere, nicht abgefragte Begriffe zusätzliche Vorgabedokumente bringen können.

Für den Aufwand, der an **Nachweisdokumenten** für die Umsetzung bestimmter Anforderungen oder ihrer Überprüfungen zu dokumentieren ist, liefert ebenfalls ein Filtern der in der XML-Version des IT-Grundschutzes enthaltenen Kompendium-Anforderungen einen Hinweis: 307 Anforderungen enthalten das Schlüsselwort „dokumentiert“ oder „dokumentieren“. Eine genaue inhaltliche Betrachtung, was sie dokumentieren und eine Bereinigung um eventuelle Redundanzen ist im Rahmen dieser Arbeit nicht erfolgt und verspricht auch keine hilfreichen Erkenntnisse. Es erscheint sehr plausibel, den Aufwand für das Dokumentieren verschiedenster Anforderungen, Überprüfungen etc. als fragwürdig hoch, in der Größenordnung von über 200, einzuschätzen.

Daneben ist die inhaltliche Anforderung und Abgrenzung verschiedener geforderter Dokumente untereinander oft nicht klar definiert. Zwei auffallende Beispiele für die Erstellung von Dokumenten mit ähnlichen oder sich überschneidenden Inhalten sind:

- Acht verschiedene Dokumente, die der Baustein NET.1.1 Netzarchitektur und -design vorgibt – hier wäre auf jeden Fall eine Vereinfachung für kleine Organisationen mit einfacher Architektur sinnvoll:

Dokumenten-Typ	**Thema**	**Anforderung**
Richtlinie	Netz	NET.1.1.A01
Spezifikation	Netzanforderungen	NET.1.1.A03
Konzept	DMZ-Segmentierung	NET.1.1.A10
Architektur	Netzzonen	NET.1.1.A16
Spezifikation	Netzdesign	NET.1.1.A17
Konzept	Segmentierungskonzept	NET.1.1.A22
Planung	Fein- und Umsetzungsplanung für Netzarchitektur und -design	NET.1.1.A25
Spezifikation	Betriebsprozesse für das Netz	NET.1.1.A26

Tabelle 2: Im Grundschutz-Baustein NET.1.1 erforderliche Vorgabedokumente
Quelle: [21]

- Sechs verschiedene Dokumente, die für mobile Geräte zu erstellen sind:

Dokumenten-Typ	Thema	Anforderung
Richtlinie	Clients	SYS.2.1.A09
Konzept	Verschlüsselung von Clients	SYS.2.1.A28
Richtlinie	Laptops	SYS.3.1.A06
Richtlinie	Smartphones und Tablets	SYS.3.2.1.A0
Richtlinie	Nutzung von mobilen Geräten	SYS.3.2.1.A1
Richtlinie	Nutzung von Mobiltelefonen	SYS.3.3.A01

Tabelle 3: Im Grundschutz vorgesehene Vorgabedokumente für mobile Clients
Quelle: [21]

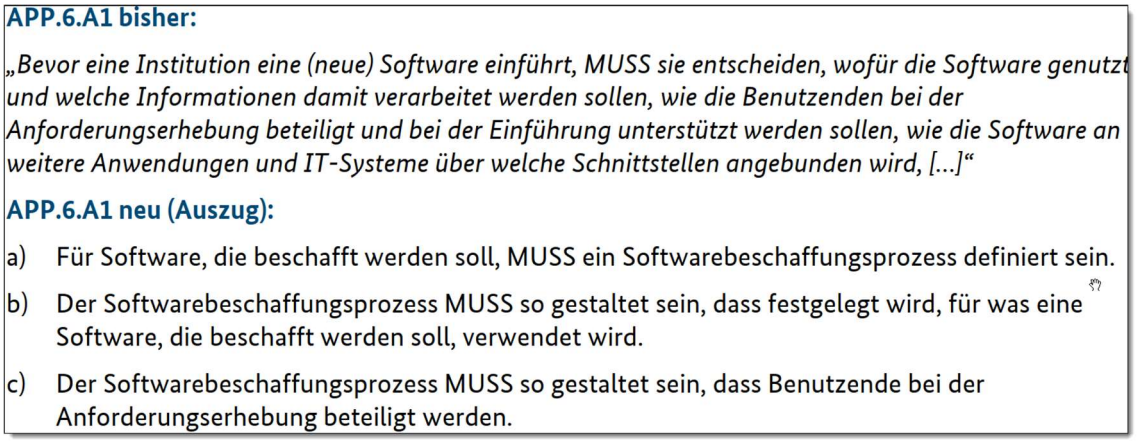
4.3.6 Überarbeitungspläne des BSI

Das BSI hat selbst eine grundlegende Überarbeitung des IT-Grundschutzes angekündigt [35], deren Aspekte – soweit öffentlich bekannt – eine kritische Würdigung im nächsten Abschnitt berücksichtigt und hier zusammengefasst sind.

Eine **Neuformulierung aller Anforderungen** in den Kompendium-Bausteinen ist der erste dabei wichtige Aspekt; dies beinhaltet:

- Untergliederung der Anforderungen in nummerierte Teilanforderungen mit jeweils einem Aspekt
- Sprachliche Vereinheitlichung, idealerweise anhand von schablonenartigen, stets ähnlich formulierten Sätzen
- Fokussierung auf überprüfbare Ergebnisse
- Reduzierung des Textumfangs.

Zur Veranschaulichung hat das BSI folgendes Beispiel veröffentlicht:



APP.6.A1 bisher:

„Bevor eine Institution eine (neue) Software einführt, MUSS sie entscheiden, wofür die Software genutzt und welche Informationen damit verarbeitet werden sollen, wie die Benutzenden bei der Anforderungserhebung beteiligt und bei der Einführung unterstützt werden sollen, wie die Software an weitere Anwendungen und IT-Systeme über welche Schnittstellen angebunden wird, [...]“

APP.6.A1 neu (Auszug):

a) Für Software, die beschafft werden soll, MUSS ein Softwarebeschaffungsprozess definiert sein.

b) Der Softwarebeschaffungsprozess MUSS so gestaltet sein, dass festgelegt wird, für was eine Software, die beschafft werden soll, verwendet wird.

c) Der Softwarebeschaffungsprozess MUSS so gestaltet sein, dass Benutzende bei der Anforderungserhebung beteiligt werden.

Abbildung 11: Beispiel für die geplante Überarbeitung von Grundschutz-Anforderungen Quelle: [35]

Die **Reduzierung von Dokumentationsaufwänden** ist der zweite Hauptaspekt der Überarbeitung mit u. a. folgenden möglichen Teilaktivitäten:

- Vorgabe einer „Dokumentenpyramide“, die erforderliche Dokumentation in bestimmte Dokumenten-Typen wie strategische, taktische, operative Dokumente gliedert und Hinweise zu Formaten gibt.
- Erläuterungen und Übersichten zu allen Dokumentationsaufwänden
- Konsolidierung und Zusammenführung von Dokumentationsaufwänden.

Daneben ist es beabsichtigt, für einen leichteren Einstieg in den IT-Grundschutz den „Weg in die Basis-Absicherung“ zu fördern.

4.3.7 Kritische Würdigung des IT-Grundschutz

Geplante Überarbeitung des IT-Grundschutzes vom BSI

Die beschriebene laufende Überarbeitung durch das BSI greift einige berechtigte Kritikpunkte auf, besonders relevant erscheinen:

- Das Aufbrechen von Anforderungen im Grundschutz-Kompendium in nummerierte Teilanforderungen erleichtert erheblich das systematische Nachverfolgen der mitunter sehr unterschiedlichen Teilaspekte. Damit übernimmt das BSI eine in der Praxis gängige Arbeitshilfe direkt in das Kompendium.

- Die angestrebte Fokussierung auf ein prüfbares Ergebnis – sofern es denn zum sinnvollen Verschärfen oder Entfallen diverser Anforderungen führt. Ein gutes Beispiel ist die mehrfach im Zusammenhang mit Richtlinien anzutreffende Formulierung, dass sie „… grundlegend für die Arbeit …“ sein sollte.
- Reduzierung des Dokumentationsaufwands, dieses Ziel ist nach der Diskussion in 4.3.5 uneingeschränkt zu unterstützen, insbesondere für Anforderungen zur Erstellung mehrfacher Dokumente mit ähnlichen oder nicht klar voneinander abgegrenzten Inhalten.
  Wichtig ist dabei auch die vom BSI nicht als Priorität hervorgehobene Reduzierung der *Anzahl* zu erstellender Dokumente.

Kritisch anzumerken ist, dass in den Zielen der Überarbeitung von Anforderungstexten die **Fokussierung auf Sicherheitsaspekte** unklar ist. Sie könnte zu einer Verschlankung des Textumfangs führen und das BSI nennt sie als einen Aspekt unter vielen, in dem bisher einzigen veröffentlichten, oben zitierten Beispiel ist sie jedoch *nicht* gegeben. Siehe Anhang 0 für eine genaue Kommentierung, hier sei zur Veranschaulichung genannt:

- Die überarbeitete Beispielformulierung enthält, dass ein Software-Beschaffungsprozess definiert sein muss. Dies ist jedoch eine organisatorische Anforderung, die per se *keinen* Beitrag zur Informationssicherheit leistet. Entscheidend ist, dass bei der Software-Beschaffung Sicherheitsaspekte wie der Bezug aus vertrauenswürdigen Quellen, Prüfung auf Notwendigkeit etc. Beachtung finden.
- Die überarbeitete Beispielformulierung enthält, dass Anwender bei der Anforderungserhebung beteiligt sein *müssen*. Dies hat ebenfalls keinen Bezug zu Sicherheitsaspekten. Anwender legen aller Erfahrung nach Wert auf andere Aspekte wie Benutzerfreundlichkeit und kurze Antwortzeiten.

Aufwand

Die Reduzierung des Aufwands für Informationssicherheit ist erklärtes Ziel des IT-Grundschutzes [29, S. 8]. Das wichtigste Instrument hierfür ist Arbeitsersparnis bei der Risikoanalyse, indem der IT-Grundschutz eine standardisierte Risikoanalyse für normalen Schutzbedarf enthält und nur für

erhöhten Schutzbedarf und im Kompendium nicht abgedeckte Szenarien eigene Risikoanalysen zu erstellen sind.

Der sehr formale Ansatz mit aufwändigerer Strukturanalyse, einer großen Zahl von Grundschutz-Checks und genannten Dokumentationsaufwendungen steht dem entgegen. Haufe/Dzombeta nennen ca. 10 – 20 % *Mehr*aufwand für den IT-Grundschutz gegenüber ISO/IEC 27001, mit dem Hinweis „Formalismus kompensiert gesparte Aufwände bei den Risikoanalysen“ [28, S. Kap. 5.3]. Weitere Quellen mit vergleichbaren Angaben hat eine Recherche nicht gefunden, die zitierte Quelle erscheint aber glaubwürdig, da die Verfasser nicht nur Mitwirkende am IT-Grundschutz und ISO/IEC-Standards sind, sondern auch als Berater und Auditor für beides praktisch tätig sind.

Aufwändig sind vor allem bei größeren Informationsverbünden auch die Grundschutz-Checks, da diese je Anforderung und Zielobjekt durchzuführen sind und so schnell eine sehr hohe Zahl erreichen. Anschließend ist daraus eine Umsetzungsplanung zu erstellen. Unter Inkaufnahme einer etwas weniger detaillierten Planung könnte die Abschätzung der Umsetzungslücken und des Aufwands aus einer gröberen Betrachtung erfolgen und ein Projekt direkt in die Umsetzung übergehen und so gleiche Ergebnisse mit spürbar weniger Aufwand erreichen.

Dem Vorteil eines möglicherweise geringeren Aufwandes bei ISO/IEC 27001 steht aber das Risiko einer zu oberflächlichen Anwendung gegenüber, die zu einer zu ungenügenden Detailtiefe bei realisierten Maßnahmen führen kann, wo der Grundschutz die Betrachtung aller relevanten Kompendium-Anforderungen verlangt.

Sicherheitsmaßnahmen

Bei einem detaillierten Blick in die Sicherheitsmaßnahmen fallen mehrere Punkte auf, die den Aufwand erhöhen und sich in einer gründlichen Überarbeitung verbessern ließen:

- Zahlreiche Anforderungen bringen wiederum Folgeaktivitäten und entsprechenden Aufwand mit sich, der durch eine konkretere Formulierung

oder weiteren Details direkt in der Anforderung reduzierbar wäre. Ein einzelnes, aber typisches Beispiel ist die Anforderung in APP.2.1, dass ein Verzeichnisdienst „sicher konfiguriert werden“ muss – ohne weiterführende Details der Art „… dabei ist mindestens zu berücksichtigen: …“
Anhang 0 enthält weitere Beispiele zur Veranschaulichung, um diese Aussage zu stützen.

- Die Gruppierung von technischen Objekten u. a. bei ähnlicher Konfiguration führt dazu, dass manche Bausteine des Kompendiums mehrfach in Grundschutz-Checks zu bearbeiten sind. Z. B. enthält das vom BSI selbst veröffentlichte Arbeitsbeispiel der RECPLAST neun Gruppen für unterschiedlich konfigurierte Laptops und Clients ([36], siehe dort die Modellierung für SYS.2.1 und SYS.3.1).
  Die Bausteine enthalten aber auch Anforderungen, die typischerweise nur einmalig und einheitlich umgesetzt werden; im genannten Beispiel wären dies z. B. Regelungen für Verlustmeldungen oder zur geregelten Übernahme und Rückgabe. Entsprechend sind diverse Anforderungen neun Mal identisch in den zugehörigen Grundschutz-Checks behandelt.

Ergebnisorientierte Formulierung von Anforderungen

Der IT-Grundschutz verzichtet auf eine saubere Trennung in Sicherheitsanforderungen und -maßnahmen, obwohl es im Glossar des Grundschutz-Kompendiums begrifflich vorgesehen ist (siehe 3.2). Die in den Kompendium-Bausteinen gelisteten Anforderungen enthalten viele Maßnahmen, die organisationsabhängig nicht immer sinnvoll sind, insbesondere für kleinere Unternehmen.

Die saubere Trennung von Anforderungen als zu erreichende Ergebnisse einerseits – analog zu ISO/IEC 27001 und dem später diskutierten NIST Cybersecurity Framework – von empfohlenen Maßnahmen als zugehörigen Aktivitäten andererseits würde der Anwendbarkeit insbesondere auf verschiedene Organisationsgrößen sehr dienlich sein. Dann könnten zu einer generisch formulierten Anforderung unterschiedlich abgestufte Maßnahmen als Optionen angeboten werden.

Einen Schritt in diese Richtung ist auch die einzige gefundene Übersetzung des IT-Grundschutzes aus Estland gegangen, zusammen mit dem Verzicht auf die Formulierung mit den Modalverben muss / soll (siehe 4.6.2).

Vorgehensmodell

Das Vorgehensmodell ist sehr umfangreich beschrieben, in den zwei BSI-Standards 200-1 und -2 mit zusammen über 200 Seiten, hier liegt ein massiver Unterschied zu der äußerst kompakten IS0 27001. Die Ausführlichkeit und Darstellung in zusammenhängend lesbarer Form ist grundsätzlich positiv zu sehen und im Sinne des Ziels einer Umsetzungshilfe zur ISO/IEC 27001 zu begrüßen.

Die Aufteilung in zwei Dokumente ist dem Umstand geschuldet, dass der erste Standard 200-1 ISMS kompatibel zur ISO/IEC 27001 und unabhängig von der Grundschutz-Methodik stehen soll [7, S. 12]. Ein Zusammenlegen von 200-1 und 200-2 könnte jedoch Überschneidungen bereinigen und die Dokumentation insgesamt kürzer ausfallen lassen.

Zudem sind diverse begriffliche Unschärfen (s. 4.3.3) kritisch anzumerken und die Bereinigung von Überschneidungen und Wiederholungen innerhalb des Standards 200-2 könnte auch zu einer Verkürzung beitragen.

Anpassbarkeit an Organisationen verschiedener Art und Größe

Die Anpassbarkeit für Institutionen verschiedenster Art und Größe – vom BSI selbst explizit als Ziel formuliert [29, S. 7] – ist kritisch zu sehen. Die verschiedenen Vorgehensweisen Standard-, Basis- und Kern-Absicherung variieren das Schutzniveau bzw. den Geltungsbereich des ISMS; sie sind *keine* Anpassungen an die Organisationsgröße.

Die Anforderungen in den Kompendium-Bausteinen enthalten keine Abstufungen von Maßnahmen für Organisationen unterschiedlicher Größe. Lediglich der Standard 200-1 zeigt verschiedene Abstufungen der Informationssicherheits-Organisation.

Im Lagebericht 2023 stellt das BSI selber die Eignung für Unternehmen mit weniger als 50 Beschäftigten in Frage: „Bereits existierende Standardwerke […] wie das IT-Grundschutz-Kompendium des BSI […] eignen sich eher für Unternehmen, die einen eigenständigen IT-Betrieb haben. Dies trifft auf den überwiegenden Teil der Unternehmen mit weniger als 50 Beschäftigten jedoch nicht zu.“ [37, S. 65]. Auch das IT-Grundschutz-Kompendium schreibt, dass eine eigene interne Organisationseinheit für den IT-Betrieb Voraussetzung für eine erfolgreiche Umsetzung ist [21, S. 1]. 198-mal (!) verwendet das Grundschutz-Kompendium den Begriff „IT-Betrieb“.

Im zugrundeliegenden Standard ISO/IEC 27001 ergibt sich eine Anpassung an die Organisationsgröße automatisch mit der Auslegung der jeweiligen Anforderungen, die nur Ziele vorgeben und den Weg dorthin offenlassen. In der selbst gewählten Rolle als Umsetzungshilfe zur ISO/IEC 27001 scheint es problematisch und nicht ausreichend, keine Flexibilität in den Baustein-Anforderungen anzubieten.

Neben der fehlenden Flexibilität für kleine Organisationen ist der Ursprung im Behördenumfeld sehr sichtbar. Es taucht z. B. 83-mal der von dort stammende Begriff „fachverantwortlich“ im Grundschutz-Kompendium 2023 auf; dies ist für eine gewünschte breite Akzeptanz auch bei Unternehmen ungünstig.

Dokumentation

Der Dokumentationsaufwand im IT-Grundschutz ist kritisch zu sehen. Er ist eindeutig sehr hoch (siehe 4.3.5) und lässt zu wenig Wahlmöglichkeiten, wenn eine Organisation eine Art von Dokumentation nicht als erforderlich ansieht. Einige Aspekte wären bei der in Arbeit befindlichen Überarbeitung des Dokumentationsaufwandes über die vom BSI publizierten Vorschläge hinaus wünschenswert:

- Die Dokumentationsanforderungen orientieren sich an größeren Organisationen und vereinzelt sogar an bestimmten Projekt-Vorgehensweisen, die zu Begriffen wie „Fein- und Umsetzungsplanung“ gehören. Diese sollten jedoch nicht als allgemeingültig angenommen werden.

- Zudem sind die erwarteten Inhalte der jeweiligen Dokumente nicht klar voneinander abgegrenzt, was für die praktische Anwendung hinderlich ist und dem Ziel einer Umsetzungshilfe entgegensteht.
- Eine nicht verbindliche Empfehlung für die gesamte Dokumentenstruktur von Richtlinien zur Orientierung wäre eine große praktische Umsetzungshilfe.
- Es könnten einmalig an zentraler Stelle (z. B. als Konkretisierung von ISMS.1.A13) Anforderungen für Dokumentenlenkung und Vorgabedokumente formuliert werden. Dies fehlt bisher im Kompendium und ist im BSI-Standard 200-2, Kap. 5 nur allgemein behandelt, ohne klar formulierte, direkt umsetzbare und überprüfbare Anforderungen. Es könnten dann an vielen Stellen redundante Anforderungen, z. B., dass Richtlinien regelmäßig zu überprüfen sind, entfallen.
- Die vom BSI geplante Aufteilung der ISMS-Dokumentation in strategische, taktische und operative Dokumente lässt sich sinnvoll um die in der Audit-Praxis übliche Unterscheidung von Vorgabe- und Nachweisdokumenten ergänzen (s. auch [28, S. Kap. 2.7].
- An vielen Stellen heißt es, dass eine Richtlinie oder ein Konzept zu erstellen ist – ohne Vorgabe von dabei zu behandelnden Aspekten (siehe Beispiele in Anhang 0). Hilfreich wäre eine durchgängige Formulierung nach dem Muster von NET.1.1.A1
  - „Es muss / sollte eine Richtlinie zu … erstellt werden“
  - „Dabei sind mindestens folgende Aspekte zu behandeln: …“.

4.4 Österreichisches Informationssicherheitshandbuch

4.4.1 Überblick

Das österreichische Informationssicherheitshandbuch [38] hat zum Ziel, bei der Erstellung eines ISMS und allen Aspekten der Informationssicherheit zu helfen. Es sieht sich als Implementierungshilfe zur ISO/IEC 27001, daneben als Instrument zur Schulung und Weiterbildung und als ein ganzheitliches Werk zur Informationssicherheit (ebd. S. 32 f.).

Es ist ein umfangreiches Dokument mity rund 800 Seiten, das zum einen die Methodik eines ISMS beschreibt, angelehnt an den IT-Grundschutz, und zum anderen sehr ausführliche Erläuterungen zu möglichen Sicherheitsmaßnahmen gibt, strukturiert wie im Anhang A der ISO/IEC 27001:2013. Damit verfolgt es einen ähnlichen Ansatz wie der IT-Grundschutz, übernimmt aber nicht dessen Baustein-Struktur und gibt im IT-Grundschutz nicht vorhandene Empfehlungen für Vereinfachungen bei kleinen Organisationen. Ferner hat es ebenfalls seinen Ursprung in der Verwendung für die öffentliche Verwaltung und ist erst später an die Bedürfnisse der Wirtschaft angepasst worden.

4.4.2 Inhaltliche Beschreibung

Das österreichische Informationssicherheitshandbuch ist in Form eines PDF-Dokumentes veröffentlicht [38]. Zusätzlich existiert eine Webseite, die alle Inhalte identisch wiedergibt sowie einfache Filterfunktionen und einzelne Checklisten ergänzt [39].

Die Kapitelstruktur ist zweigeteilt, analog zum IT-Grundschutz und ISO/IEC 27001/27002:

- Kap. 2 – 5 beschreiben den Aufbau eines ISMS mit seiner Methodik, Grundlagen und dem Vorgehen zur Risikoanalyse
- Kap. 6 – 18 diskutieren und erläutern mögliche Sicherheitsmaßnahmen, in einer Gliederung wie der Anhang A der ISO/IEC 27001:2013 und Kap. 6 – 18 der ISO/IEC 27002:2013.

Vorgehensweise gemäß Kap. 2 – 5

Das Vorgehen zur Erstellung eines ISMS ist in einer eigenständigen Darstellung beschrieben, inhaltlich aber bis auf die Behandlung der Risikoanalyse weitgehend deckungsgleich mit der IT-Grundschutz-Methodik.

Abbildung 12: Wesentliche Prozessschritte zur Umsetzung und Verwendung eines ISMS
Quelle: [38, S. 43]

Der Ansatz des IT-Grundschutz, bei normalem Schutzbedarf auf eine eigene Risikoanalyse zu verzichten und stattdessen auf einer standardisierten Risikoanalyse basierende vordefinierte Schutzmaßnahmen zu übernehmen, ist im österreichischen Ansatz eine Wahlmöglichkeit. Dies zeigt sich im ebenfalls an den IT-Grundschutz angelehnten „Informationssicherheitsmanagementprozess“, der in Begrifflichkeiten und der Darstellung eigenständig ist, inhaltlich aber dem Sicherheitsprozess des IT-Grundschutzes entspricht.

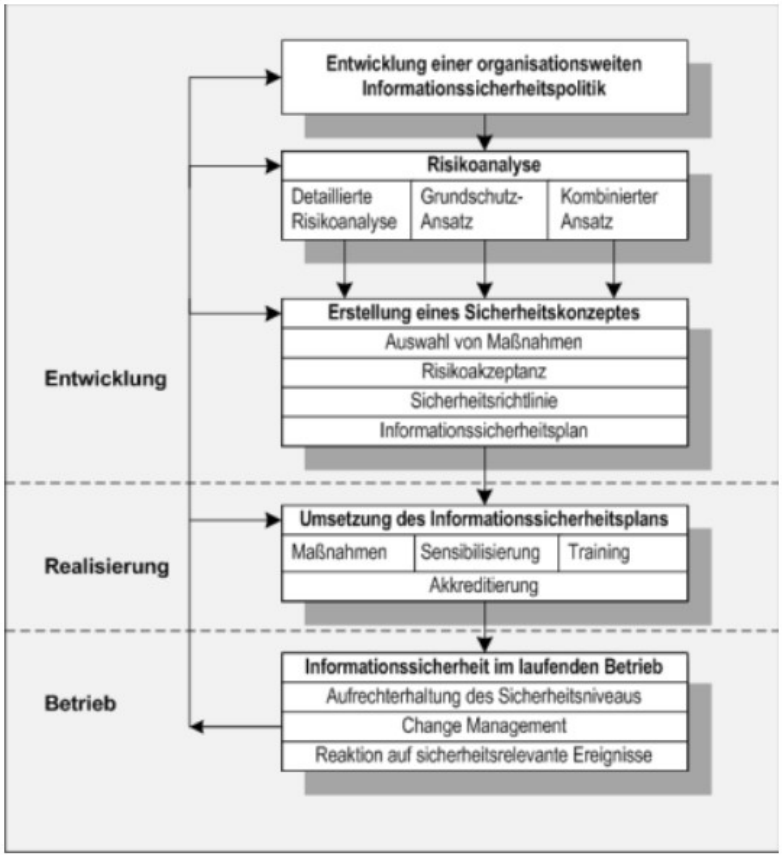


Abbildung 13: Der Informationssicherheitsmanagementprozess des österreichischen Informationssicherheitshandbuchs
Quelle: [38, S. 73]

Das zentrale Ergebnis dieses Prozesses ist ein sog. Informationssicherheitsplan, der alle vorhandenen und geplanten Sicherheitsmaßnahmen sowie einen Umsetzungsplan und eine Bewertung der Restrisiken enthält [38, S. 85].

Die Optionen bei der Wahl der Risikoanalyse bedeuten:

- Detaillierte Risikoanalyse: Durchführung einer Risikoanalyse mit individueller Auswahl von Maßnahmen für alle IT-Systeme; hierfür verweist das Handbuch wiederum u. a. auf ISO/IEC 27002 und den IT-Grundschutz
- Grundschutz-Ansatz: Verzicht auf Risikoanalyse, Auswahl einer pauschalierten Gefährdungslage und direkte Auswahl sogenannter Grundschutzmaßnahmen
- Kombinierter Ansatz: Verwendung des Grundschutz-Ansatzes für IT-Systeme mit normalem Schutzbedarf und eine detaillierte Risikoanalyse für Systeme mit erhöhtem Schutzbedarf.

Der sog. „kombinierte Ansatz“ entspricht tatsächlich der Vorgehensweise des BSI-Standards 200-2 und die im IT-Grundschutz vorhandene Abstufung von Basis-Anforderungen, Standard-Anforderungen und Anforderungen für erhöhten Schutzbedarf finden sich im österreichischen Ansatz nicht wieder. In diesem Punkt ist das österreichische Sicherheitshandbuch offenbar noch nicht an den seit 2017 geltenden BSI-Standard 200-2 angepasst.

In die gleiche Richtung deuten eine Reihe von Verweisen auf die veralteten Standards 100-2 und „Grundschutz-Kataloge“, die sich noch in der Februar 2023 erschienenen Version 4.3.3 des österreichischen Informationssicherheits-handbuchs [40] fanden und in der Version 4.4.0 im November 2023 bereinigt wurden.

Sicherheitsmaßnahmen gemäß Kap. 6 – 18

Die Kapitel 6 – 18 des österreichischen Informationssicherheitshandbuchs entsprechen jeweils den Kapiteln der ISO/IEC 27002:2017 mit nur geringen Abweichungen und enthalten zu jedem Thema ausführliche, zusammenhängend lesbare Erläuterungen. Eine Liste der Kapitel mit einem Textauszug zur Veranschaulichung befindet sich im Anhang 8.1.

4.4.3 Zusammenfassende Bewertung

Das Österreichische Informationssicherheitshandbuch steht der eigenen Zielsetzung gemäß zwischen ISO/IEC 27001/27002 und dem deutschen IT-Grundschutz, sowohl im Umfang als auch in der Methodik, die mehr Freiheiten lässt als der Grundschutz. Es bietet anders als das deutsche Grundschutz-Kompendium thematisch gegliederte, zusammenhängend lesbare Erläuterungen anstelle reiner Sicherheitsmaßnahmen und wesentlich mehr Inhalte als die sehr knapp gehaltene ISO/IEC-Norm.

Die Veröffentlichung in einer Online-Plattform ist eine nachahmenswerte Form, der dadurch bisher geschaffene Mehrwert aber in der österreichischen Variante sehr gering und die Implementierung nicht auf dem Stand der Technik.

In der Vorgehensweise und den empfohlenen Sicherheitsmaßnahmen zeigt es keine wichtigen Unterschiede, die als Anregungen für den deutschen IT-Grundschutz dienen können.

Kritisch anzumerken ist der bei gewissenhafter Befolgung zu erwartende **sehr hohe Arbeitsaufwand** dieses Ansatzes:

- Der Umfang ist mit 800 Seiten sehr hoch und für große Organisationen sind alle Kapitel relevant, es ergibt sich keine Eingrenzung auf relevante Bausteine überschaubarer Größe wie in der IT-Grundschutz-Methodik und den Bausteinen des Kompendiums.
- Aus den Erläuterungen ergibt sich eine große Vielzahl von Folgeaufgaben wie die Erstellung von diversen Konzepten und Richtlinien.
- Sicherheitsmaßnahmen sind oft aus den Erläuterungen erst abzuleiten oder ohne klare Prioritäten genannt; die Ableitung von individuellen Sicherheitsmaßnahmen erfordert also einen erheblichen Arbeitsaufwand zusätzlich zum Durcharbeiten des Handbuchs. Der Abstraktionsgrad ist immer noch so hoch, dass meist keine direkt umsetzbaren Maßnahmen genannt werden, sondern immer noch eine Auslegung und Anpassung erforderlich sind.

Für vordefinierte Maßnahmen verweist das Handbuch wiederum oft auf ISO/IEC 27002 und den Grundschutz als mögliche Quellen – was wiederum erheblichen zusätzlichen Arbeitsaufwand mit sich bringt.

- Die sich bei einer Anwendung dieses Ansatzes ergebenden äußerst zahlreichen Folgearbeiten sind allesamt in langem Fließtext enthalten, daher für eine systematische Bearbeitung und Nachverfolgung aufwändig zu handhaben, ohne dass dafür geeignete Tools zur Verfügung stehen.

Eine hilfreiche Quelle kann das Werk sein, um zu ausgewählten Themen der ISO/IEC-Normen zusammenhängende und umfassende Erläuterungen nachzulesen, die in diesem Umfang und ihrer Vollständigkeit an keiner anderen Stelle bekannt sind.

Als Leitfaden für eine praktische Umsetzung, eine systematische Implementierung eines ISMS erscheint es nicht geeignet.

4.5 Schweiz: Sicherheitsverfahren

4.5.1 Überblick

Das Schweizer „Sicherheitsverfahren“ [41] legt minimale Anforderungen an die sog. „Informatiksicherheit“ der Bundesverwaltung fest. Einer seiner Bestandteile ist der „IT-Grundschutz in der Bundesverwaltung“.

Es ist ein nationaler Standard, verpflichtend für die Schweizerische Bundesverwaltung. Obwohl es keinen Anspruch formuliert, auch für Unternehmen anwendbar zu sein, soll es wegen der Zusammenarbeit zwischen deutschen, österreichischen und Schweizer Behörden sowie der Namensgleichheit trotzdem betrachtet werden.

Das Auffälligste an diesem Ansatz ist seine Kürze. Die maßgebliche Webseite hat nur vier Unterseiten; das Verfahren ist in drei Dokumenten mit zusammen nur 45 Seiten beschrieben. Inhaltlich sind die Maßnahmen „teilweise aus ISO/IEC 27002 entnommen“ und „in Anlehnung an ISO/IEC 27002 strukturiert“ [42, S. 8].

4.5.2 Inhaltliche Beschreibung

Das Schweizer Sicherheitsverfahren basiert auf einer separaten Betrachtung und Absicherung einzelner „Informatikschutzobjekte“. Dies ist ein Begriff aus der Schweizer Cyberrisikenverordnung (CyRV) und entspricht dem „Zielobjekt“ im deutschen IT-Grundschutz. Der Schweizer Ansatz sieht aber nicht nur vor, mehrere gleiche, sondern auch *zusammenhängende* Objekte zu einem Informatikschutzobjekt zusammenzufassen, also z. B. ein gesamtes Netzwerk als ein Informatikschutzobjekt zu betrachten.

Die konkrete Festlegung und Abgrenzung von Informatikschutzobjekten sind nicht vorgegeben. Es muss lediglich für jedes Schutzobjekt ein Verantwortlicher definiert sein und die Zusammenfassung von Schutzobjekten ist auf „inhaltlich zusammengehörende“ mit gleichem Schutzbedarf beschränkt [42, S. 4].

Vorgehensweise

Die Vorgehensweise ist folgende:

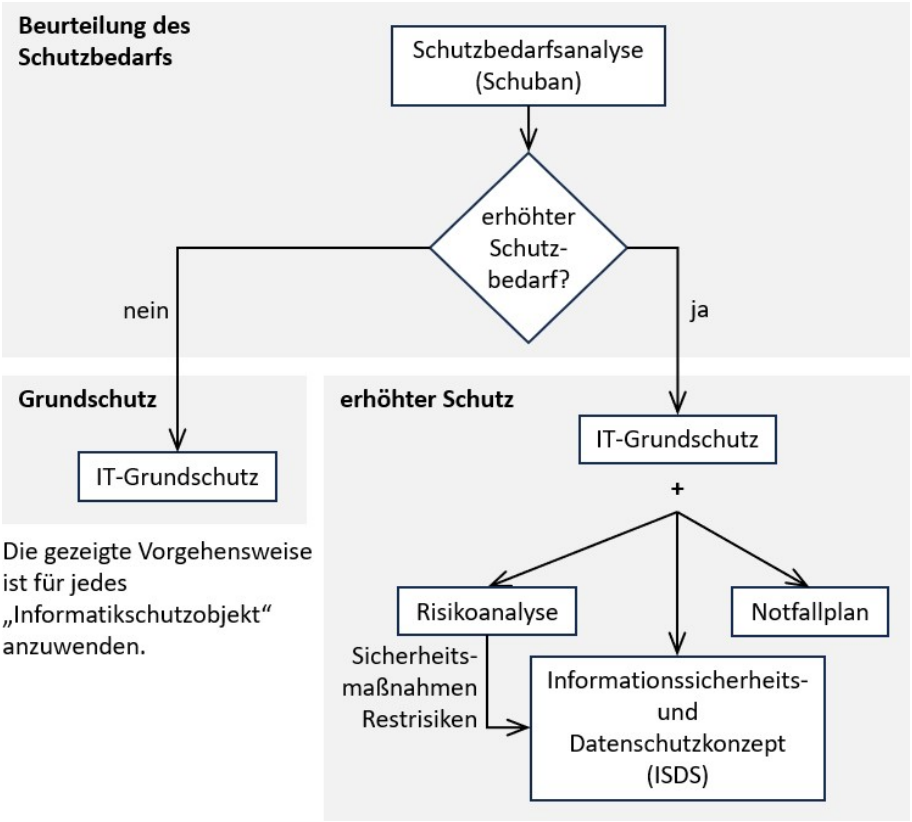


Abbildung 14: Vorgehensweise des Schweizer Sicherheitsverfahrens
Quelle: Eigene Darstellung, basierend auf [41]

- Für jedes Schutzobjekt ist eine **Schutzbedarfsanalyse** [43] vorzunehmen. Sie prüft anhand einfacher Fragen den Schutzbedarf hinsichtlich Vertraulichkeit, Verfügbarkeit, Integrität sowie zusätzlich Nachvollziehbarkeit und eventuelle nachrichtendienstliche Relevanz. Das Ergebnis ist ein pauschal erhöhter oder nicht erhöhter Schutzbedarf.
- Sofern **kein erhöhter Schutzbedarf** vorliegt, ist eine Absicherung nach *IT-Grundschutz* [42] ausreichend, Details folgen weiter unten.
- Bei **erhöhtem Schutzbedarf** ist zusätzlich ein detaillierteres *Informations- und Datenschutzkonzept (ISDS)* zu erstellen. Es nimmt aus einer Risikoanalyse abgeleitete zusätzliche Maßnahmen auf und dokumentiert alle Arbeitsschritte und -ergebnisse sowie Restrisiken. Konkrete zusätzliche Sicherheitsmaßnahmen sind jedoch für erhöhten Schutzbedarf nicht in Form eines Kataloges oder einer Liste vorgegeben. Daneben ist ein Notfallplan zu erstellen. Für alle drei Dokumente sind einfache Vorlagen verfügbar.

Sicherheitsmaßnahmen im Schweizer „IT-Grundschutz“

Der Schweizer IT-Grundschutz legt zunächst Grundsätze und Prinzipien fest, die für alle Schutzobjekte zu erfüllen sind [42, S. 7]:

- **„Zero Trust“-Prinzip** sollte nach Möglichkeit erfüllt sein
- **„Defense-in-Depth“-Prinzip** muss „wenn möglich und wirtschaftlich vertretbar“ mit sich gegenseitig ergänzenden Sicherheitsmaßnahmen erfüllt sein – „präventiv, detektiv und reaktiv“.
- Alle eingesetzten Sicherheitsmaßnahmen müssen dem **Stand der Technik** entsprechen.
- Die Vergabe von Zugriffsrechten und Privilegien muss nach **„Least Privilege“-** bzw. **„need-to-know“-Prinzip** minimal erfolgen.
- Die Entwicklung von Hard- und Softwarekomponenten muss das **„Security by Design“-Prinzip** einhalten.
- Entwicklung und Konfiguration von Schutzobjekten muss nach dem **„Security by Default“-Prinzip** alle sinnvollen Sicherheitsmaßnahmen standardmäßig aktivieren.

Daneben definiert der Schweizer IT-Grundschutz eine übersichtlich kurze, aber wegen ihres hohen Abstraktionsniveaus sehr breite Palette von Maßnahmen. Die

von ihr abgedeckten Themen sind im Anhang 0 aufgelistet. Neben wenigen relativ konkreten Vorgaben z. B. zu Passwörtern und dem Schutz vor Schadsoftware sind viele so gehalten, dass sie recht große Themenfelder eröffnen, die eine Vielzahl von weitergehenden Maßnahmen verlangen, z. B. eine generelle Forderung des Betriebs nach „branchenüblichen Sicherheitsvorgaben“ oder des Schutzes von Vertraulichkeit und Integrität „mit Hilfe kryptografischer Verfahren“.

Die folgende Tabelle fasst die Anzahl der Sicherheitsanforderungen zusammen:

Anwendungsbereich	Anzahl Themen	Anzahl Anforderungen
Organisation	4	5
Personal	2	3
Technik	8	20
Informationen	4	6
IT-Systeme	6	16
Anwendungen	2	3
Zonen (Netzwerke)	5	11
gesamt	**31**	**64**

Tabelle 4: Anzahl Sicherheitsanforderungen im Schweizer IT-Grundschutz
Quelle: Eigene Auswertung

Ferner verweisen einige Anforderungen offenbar auf in der Schweiz zentral festgelegte und umgesetzte Sicherheits-Praktiken in Form eines einheitlichen Zonenmodells für die Netze der Bundesverwaltung und damit verbundenen konkreten Zugriffsregelungen und Authentifizierungen.

4.5.3 Zusammenfassende Bewertung

Zum Begriff „IT-Grundschutz“

Der Schweizer Ansatz enthält einen wesentlichen Grundgedanken des deutschen IT-Grundschutzes: Die Reduzierung des Aufwands für Risikoanalysen durch Vorgabe eines standardisierten Katalogs von grundlegenden Sicherheitsmaßnahmen für normalen Schutzbedarf und Beschränkung der Risikoanalyse auf Objekte mit erhöhtem Schutzbedarf.

Genau betrachtet ist hier ein „IT-Grundschutz“ in seiner wörtlichen Bedeutung umgesetzt: Nur der für Objekte ohne erhöhten Schutzbedarf geltende Teil des Schweizer Sicherheitsverfahrens ist als „IT-Grundschutz“ bezeichnet. Der deutsche Ansatz des BSI bezeichnet seine gesamte Methodik als „IT-Grundschutz“, was auch Risikoanalysen sowie individuelle und vordefinierte Maßnahmen für erhöhten Schutzbedarf beinhaltet – und damit Elemente, die über einen grundlegenden Schutz hinausgehen.

Vereinfachte Vorgehensweise

Die in der weiter oben veranschaulichten Vorgehensweise erreichte Vereinfachung ist drastisch und sollte Ansporn sein, zu betrachten, wie weit und unter welchen Bedingungen Abkürzungen auf die deutsche Grundschutz-Methodik übertragbar sind. Die spätere vergleichende Betrachtung über alle verschiedenen Ansätze hinweg greift diesen Punkt auf (s. 5.5)

In seiner Einfachheit ist die Vorgehensweise unmittelbar einleuchtend, daher ohne Vorkenntnisse anzuwenden und in dieser Hinsicht ganz anders geartet als der deutsche Grundschutz.

Verkürzte Maßnahmenliste

Die sehr kurze Liste von Sicherheitsanforderungen erinnert an ein radikal verkürztes Konzept der deutschen Grundschutz-Bausteine:

- Analog zu den Prozessbausteinen ist ein kleiner Satz von Anforderungen für Organisation, Personal, Technik und Informationen immer zu erfüllen.
- Analog zu den Systembausteinen ist ein kleiner Satz von Anforderungen für IT-Systeme, Anwendungen und Zonen (Netzwerke) nur zu erfüllen, wenn für die jeweiligen Schutzobjekte relevant.

Die geringe Anzahl von Maßnahmen ist mehr Ausdruck der offensichtlich beabsichtigten Kompaktheit als von inhaltlichen Differenzen. Die Maßnahmen decken eine große Breite ab und befinden sich auf einem der ISO/IEC 27001 vergleichbaren Abstraktionsniveau. Ihre Anzahl ist mit 64 nicht allzu weit entfernt von den 93 im Anhang A der ISO/IEC 27001, die Differenz erscheint für das Ziel eines *Grund*schutzes und damit naturgemäß einer Teilmenge plausibel.

Wie ISO/IEC 27001 erfordert daher der Schweizer IT-Grundschutz zusätzliche Umsetzungshinweise, hinzu kommen die verpflichtenden Design-Prinzipien, die weitreichende Folgen haben und entsprechende Aufwände für ihre Umsetzung mitbringen.

Im Ergebnis sind damit bei gewissenhafter Anwendung de facto ähnlich umfangreiche Maßnahmen nötig wie bei ISO/IEC 27001.

Übertragbarkeit des Ansatzes

Als zentraler Ansatz für die staatliche Bundesverwaltung eines deutlich kleineren Landes wie die Schweiz ist eine Übertragbarkeit natürlich fragwürdig. Zudem greift das Schweizer Sicherheitsverfahren mit Verweisen auf „Bundesclients“ und Zonenmodelle aus einer standardisierten Netzwerkarchitektur auf wesentliche in der gesamten Verwaltung vereinheitlichte Elemente zu, die spezifisch für die Schweizer Bundesverwaltung sind.

Er beinhaltet aber die wichtige Idee eines modularen Ansatzes von Sicherheitsarchitekturen und -konzepten: Zentrale Festlegung und Steuerung von Aspekten wie Netzwerksicherheit und Endgeräteverwaltung, dezentrale Verantwortung für andere Teile wie lokal verwendete Anwendungen und Daten.

4.6 Estland: Estonian Information Security Standard (E-ITS)

4.6.1 Überblick

Der estnische Informationssicherheits-Standard E-ITS [44] hat zum Ziel, die Informationssicherheit in Estland für private wie öffentliche Organisationen zu fördern.

Er ist de facto eine Übersetzung des deutschen BSI-Standards ins Estnische und ebenso kompatibel zu ISO/IEC 27001. Er ist dort verpflichtend für öffentliche Einrichtungen und 2023 als Nachfolger des „IT baseline security system ISKE“ eingeführt. Der Vorgänger ISKE war seit 2003 der estnische Standard und begann damals mit dem zu der Zeit gültigen IT-Grundschutz des BSI [45].

4.6.2 Inhaltliche Beschreibung

Die zugehörige Webseite ist nur auf Estnisch verfügbar [46], der Versuch einer automatisierten Übersetzung dafür hat sich als nicht brauchbar erwiesen (siehe Anhang 0).

Die Schlüsseldokumente lassen sich aber trotzdem identifizieren und eine automatisierte Übersetzung mit DeepL zeigt, wie Estland bei seiner Adaption des BSI-Standards vorgegangen ist.

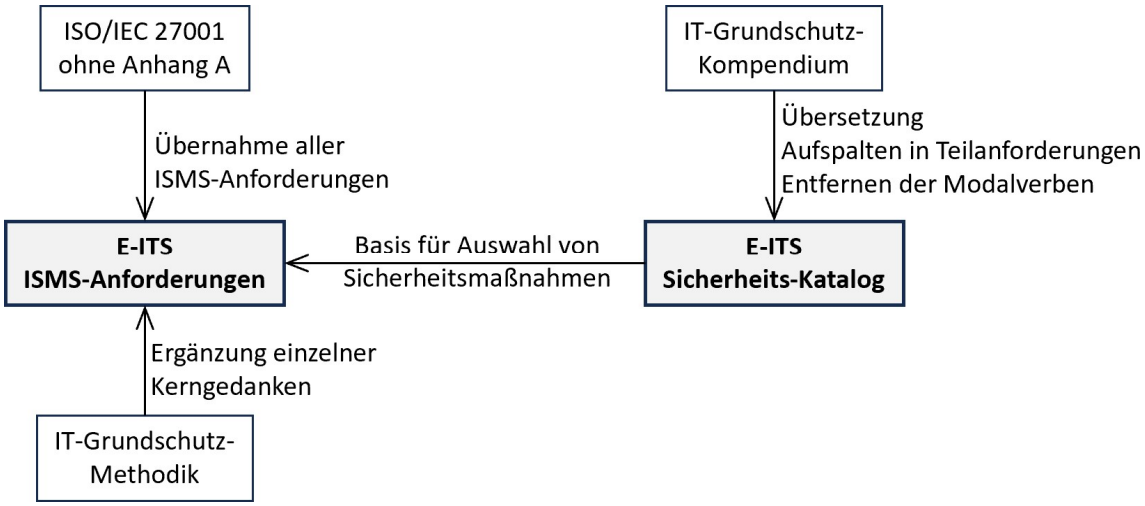


Abbildung 15: Schlüsseldokumente des estnischen Informationssicherheitsstandards E-ITS
Quelle: eigene Darstellung

Das erste Schlüsseldokument beschreibt den Aufbau eines ISMS. Es ist ein PDF-Dokument von 27 Seiten, betitelt „Estnischer Standard für Informationssicherheit – Anforderungen an das Informationssicherheits-Managementsystem“ [47]. Es ist vergleichbar der ISO/IEC 27001, mit ähnlichen Inhalten und verwandter Kapitelstruktur; beispielhafte Ausschnitte sind im Anhang 0.

Daneben gibt es einen umfangreichen Katalog von Sicherheitsmaßnahmen mit über 500 Seiten [48]. Er ist eine Übersetzung des deutschen IT-Grundschutz-Kompendiums mit sehr enger Übereinstimmung:

- identische Struktur von Bausteinen
- identische Struktur innerhalb der Bausteine – Beschreibung, Bedrohungen, Maßnahmen

- insgesamt eine fast gleiche Zahl von Maßnahmen, wie sich an der in Excel veröffentlichten Fassung verifizieren lässt; eine geringe Abweichung (1745 Anforderungen in der estnischen Fassung, 1835 im deutschen Kompendium von 2023) kann durch unterschiedliche Versionsstände bedingt sein
- übereinstimmende Unterscheidung der Anforderungen innerhalb der Bausteine in Basis-Anforderungen, Standard-Anforderungen und erweiterte Anforderungen.

Eine Prüfung von Stichproben zeigt eine inhaltlich sehr enge Übereinstimmung.

Auffallend sind folgende Abweichungen in der Übersetzung:

- Alle Anforderungen sind in klar nummerierte und dadurch leichter nachverfolgbare Teilanforderungen aufgespalten.
- Die Formulierung der Anforderungen verzichtet auf die Formulierung mit Modalverben „muss“ und „soll“, sondern beschreibt nur Ergebnisse.

Veranschaulichende Beispiele sind im Anhang 8.13.

Vom deutschen IT-Grundschutz des BSI übernimmt Estland damit nur das Kompendium mit allen Bausteinen und seinen Anforderungen vollständig. Das erwähnte an ISO/IEC 27001 orientierte Grundlagendokument erwähnt aber Schlüsselbegriffe der deutschen IT-Grundschutz-Methodik wie „Basis, Standard, Kern“.

Eine dem Anhang A von ISO/IEC 27001 vergleichbare Liste von Sicherheitsmaßnahmen gibt es nicht. Der estnische Standard spricht stattdessen davon, dass alle relevanten Module des Sicherheits-Katalogs zu berücksichtigen sind, eine Nichtaufnahme ist zu begründen. Analog sind Basisanforderungen mit Priorität umzusetzen. Der Ausschluss von Anforderungen ist zu begründen – aber damit anders als im deutschen IT-Grundschutz möglich.

4.6.3 Zusammenfassende Bewertung

Estland hat sich 2023 mit seinem neuen Standard E-ITS erneut am deutschen IT-Grundschutz orientiert. Nach 20 Jahren Erfahrung mit dem ebenfalls auf dem

deutschen IT-Grundschutz basierenden Vorgänger spricht dies für gute Erfahrungen mit dem deutschen Ansatz.

Bei der Adaption verzichtet Estland jedoch vollständig auf die IT-Grundschutz-Methodik und verwendet stattdessen ein der ISO/IEC 27001 ähnliches Dokument zur Beschreibung der Anforderungen an ein ISMS, gemäß der Zielsetzung, mit ISO/IEC 27001 kompatibel zu sein und in einer drastischen Verkürzung des deutschen Ansatzes.

Estland übernimmt das deutsche Grundschutz-Kompendium vollständig, es bekommt die Rolle des Anhangs A von ISO/IEC 27001 und ISO/IEC 27002. Dabei verzichtet es aber auf die Einteilung in MUSS- und SOLL-Anforderungen und ermöglicht wie der ISO/IEC-Standard eine Abweichung von den vordefinierten Anforderungen. Eine solche ist risikobasiert zu begründen, aber dann zulässig.

Wichtige Teile der IT-Grundschutz-Methodik stecken in einzelnen Sätzen des kurzen Grundlagen-Dokumentes wie die Möglichkeit, ein Basis- oder Standard-Niveau der Sicherheit zu erreichen und die Notwendigkeit einer Risikoanalyse bei hohem Schutzbedarf.

4.7 Deutschland: VdS 10000 und 10005

4.7.1 Überblick

Die von der deutschen Versicherungswirtschaft getragene VdS Schadenverhütung GmbH hat als VdS 10000 [50] eine vereinfachte Richtlinie für den Aufbau eines ISMS herausgegeben. Sie richtet sich an kleine und mittlere Unternehmen (KMU) und ist von der ISO/IEC 27001 abgeleitet. Es ist eine Zertifizierung dafür möglich.

Der Ansatz ist auf 43 Seiten überschaubar kurz beschrieben und besteht in seinem Hauptteil aus Anforderungen, die in sehr kurze Abschnitte klar gegliedert sind und ähnlich wie im Grundschutz mit hervorgehobenen Modalverben („MUSS“, „SOLLTE“ etc.) formuliert sind.

VdS 10005 [51] ist eine weitere Verkürzung für Klein- und Kleinstunternehmen.

4.7.2 Inhaltliche Beschreibung VdS 10000

Abgedeckte Themen und unterstützende Angebote

Die VdS 10000 ist so verfasst, dass sich aus einem kompakten Hauptdokument direkt alle erforderlichen Aktivitäten ableiten lassen, ohne Zweiteilung wie bei ISO/IEC in 27001 und 27002 oder Grundschutz-Methodik und -Kompendium.

Sie deckt folgende Themen ab:

- **Organisation**
  - Gesamtverantwortung des Topmanagements
  - Definition von Verantwortlichkeiten, insb. ISB
- **Informationssicherheits-Leitlinie**
- **Richtlinien zur Informationssicherheit**
  - Anforderungen an Richtlinien
  - Empfehlung für 7 themenspezifische Richtlinien
- **Mitarbeiter**:
  - Einweisung und Verpflichtung zur Informationssicherheit
  - Verfahren vor Aufnahme und bei Beendigung oder Wechsel einer Tätigkeit
- **Wissen**
  - Beobachten des Umfelds z. B. über Gefährdungen und rechtliche Änderungen
  - Schulung und Sensibilisierung
- **IT-Systeme**: Gängige Schutzmaßnahmen für alle Systeme wie Softwareaktualisierungen, Schutz vor Schadsoftware etc.
- **Netzwerke und Verbindungen**: Gängige Schutzmaßnahmen wie Segmentierung, Deaktivierung nicht benötigter Zugänge
- **Mobile Datenträger**
- **Umgebung**: Physische Sicherheit
- **IT-Outsourcing und Cloud Computing**
- **Zugänge und Zugriffsrechte**
- **Datensicherung und Archivierung**
- **Störungen und Ausfälle**
- **Sicherheitsvorfälle**

Ergänzend zum erwähnten Hauptdokument der VdS 10000 gibt es unterstützende Angebote [52]:

- einen „Quick Check“ in Form einer Bewertung anhand eines Online-Fragebogens für wenige Euro
- ein automatisierter Sicherheits-Scan für das Prüfen der Netzwerksicherheit von außen für rund 100 Euro
- ein „Quick Audit“ für rund 2.000 Euro.

Vorgehensweise

Der Ansatz der VdS 10000 ist so beschrieben, dass das Hauptdokument direkt für eine Umsetzung verwendet werden kann. Aus seiner Gliederung ergibt sich intuitiv das folgende Vorgehen:

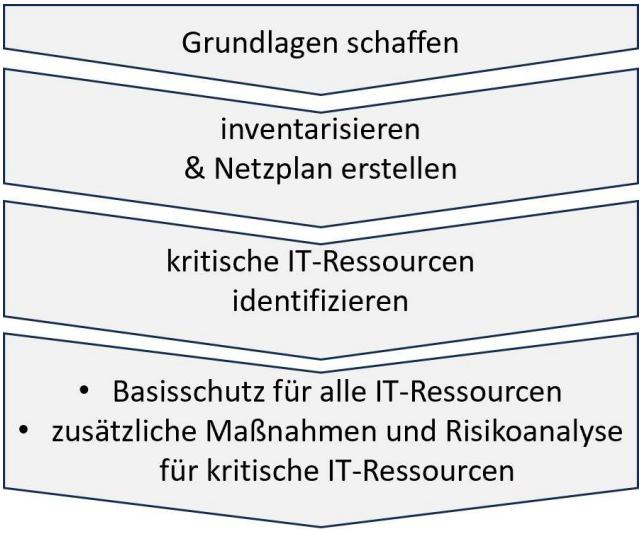


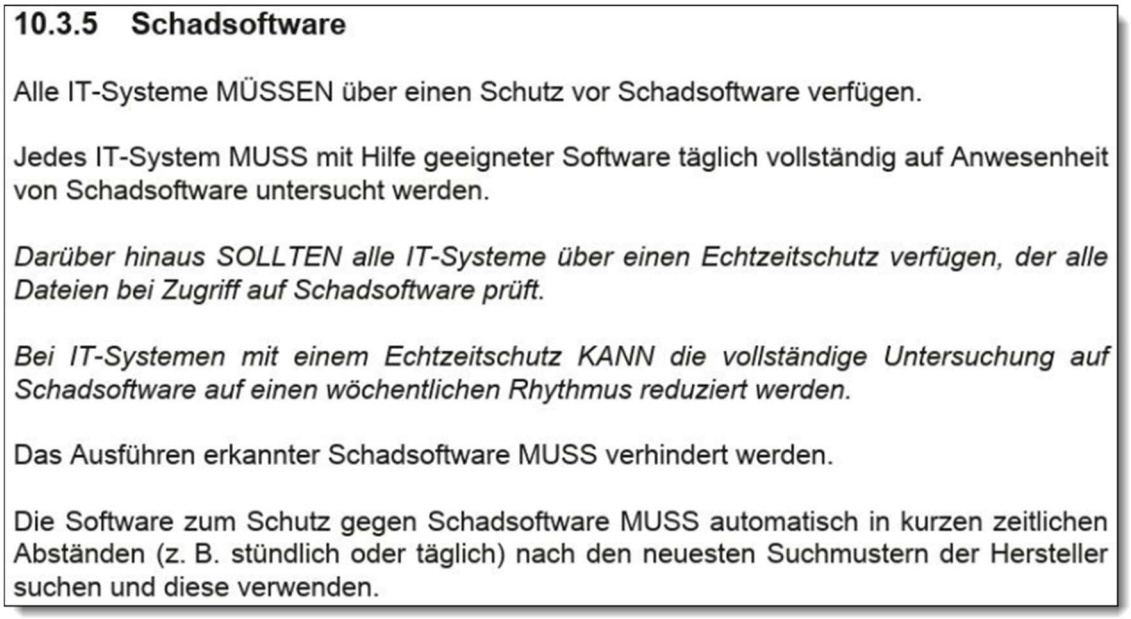
Abbildung 16: Vorgehensweise der VdS 10000
Quelle: Eigene Darstellung, basierend auf [50]

Die Grundlagen enthalten die oben genannten Themen Organisation, Informationssicherheits-Leitlinie und -Richtlinien – aus ISO/IEC 27001 und dem IT-Grundschutz bekannte Elemente. Die weiteren Schritte sind eine pragmatische Vereinfachung der komplexen Grundschutz-Methodik für kleine und mittlere Organisationen.

Sicherheitsmaßnahmen

Die in der VdS 10000 enthaltenen Maßnahmen decken eine ähnliche Breite wie ISO/IEC 27001 ab, dies zeigen bereits die zuvor gelisteten Themen. Für jedes einzelne Thema enthält sie nur eine kleine Zahl wesentlicher Anforderungen, ergebnisorientiert formuliert und in ihrem Abstraktionsgrad unter dem der ISO/IEC 27001, so dass der direkte Übergang zur Umsetzung wesentlich leichter fällt.

Zur Veranschaulichung hier ein Ausschnitt, die Basisabsicherung in Bezug auf Schadsoftware:



10.3.5 Schadsoftware

Alle IT-Systeme MÜSSEN über einen Schutz vor Schadsoftware verfügen.

Jedes IT-System MUSS mit Hilfe geeigneter Software täglich vollständig auf Anwesenheit von Schadsoftware untersucht werden.

Darüber hinaus SOLLTEN alle IT-Systeme über einen Echtzeitschutz verfügen, der alle Dateien bei Zugriff auf Schadsoftware prüft.

Bei IT-Systemen mit einem Echtzeitschutz KANN die vollständige Untersuchung auf Schadsoftware auf einen wöchentlichen Rhythmus reduziert werden.

Das Ausführen erkannter Schadsoftware MUSS verhindert werden.

Die Software zum Schutz gegen Schadsoftware MUSS automatisch in kurzen zeitlichen Abständen (z. B. stündlich oder täglich) nach den neuesten Suchmustern der Hersteller suchen und diese verwenden.

Abbildung 17: Beispiel-Anforderungen aus der VdS 10000
Quelle: [50]

4.7.3 Inhaltliche Beschreibung VdS 10005

Die VdS 10005 ist eine weitere deutliche Verkürzung der VdS 10000 für Klein- und Kleinstunternehmen auf ein Dokument von 15 Seiten. Sie ist eine reine Sammlung von Maßnahmen-Empfehlungen, ohne gesonderte Betrachtung kritischer Ressourcen, ohne Risikoanalyse.

Die Gliederung ist konsistent mit der VdS 10000, so dass es möglich ist, später dorthin aufzusteigen oder die Umsetzung punktuell mit Hinweisen von dort zu vertiefen.

4.7.4 Zusammenfassende Bewertung

In seiner Kompaktheit, Praxisnähe und intuitiven Verwendbarkeit bei gleichzeitiger Kompatibilität zur ISO/IEC 27001 erscheint der Ansatz der VdS 10000 vorbildlich als Umsetzungshilfe zur ISO/IEC 27001 für kleine und mittlere Unternehmen und ebenso die VdS 10005 für Klein- und Kleinstunternehmen.

Niedrigschwellige Zusatzangebote ergänzen beide VdS-Richtlinien sehr sinnvoll.

4.8 Polen: PPHS Cybersecurity Standard

Überblick

Der polnische „PPHS Cybersecurity Standard" [49] hat zum Ziel, einen gegenüber ISO/IEC 27001 vereinfachten Ansatz für Cybersicherheit in kleinen und mittleren Unternehmen sowie in öffentlichen Einrichtungen anzubieten. Dabei soll er Kompatibilität mit dem ISO/IEC 27001-Standard wahren, um dessen spätere Implementierung zu ermöglichen.

Er ist ein sehr anschaulich und in leicht lesbarem Text geschriebener Ansatz, der durch eine vereinfachte Fassung der wichtigsten ISO/IEC 27001-Aktivitäten führt und eine überschaubare Zahl von grundlegenden „Best Practices" als Anfangspunkt für die Auswahl von Sicherheitsmaßnahmen bereitstellt.

Inhaltliche Beschreibung

Der PPHS Cybersecurity Standard ist auf einer modern gestalteten Webseite und mit identischen Inhalten auf mehreren kleinen PDF-Dokumenten veröffentlicht. Das PPHS in seinem Namen steht für den Namen der herausgebenden Behörde.

Seine Vorgehensweise besteht aus vier einfachen Schritten, die die wichtigsten Elemente der in 4.2.2 gezeigten vollständigen Aktivitäten für den ISO/IEC 27001-Standard enthalten [50]:

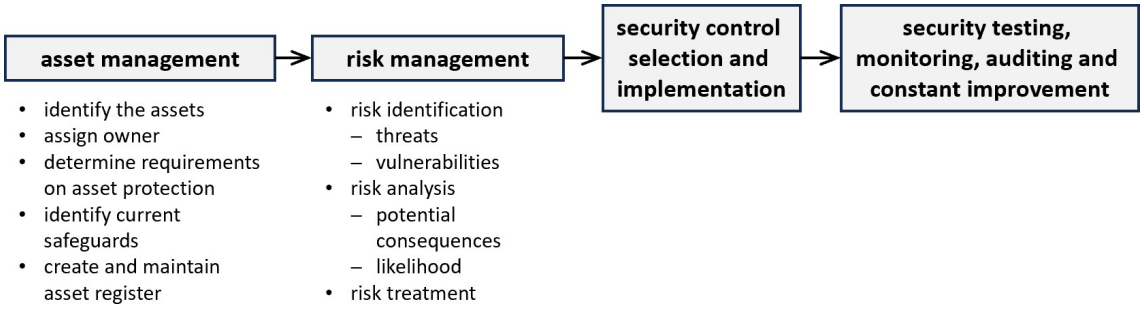


Abbildung 18: Vorgehensweise des polnischen PPHS Cybersecurity Standard
Quelle: Eigene Darstellung, basierend auf [50]

Die leicht lesbare Darstellung auf 17 Seiten führt anschaulich durch diese Schritte, allerdings ohne tiefergehende praktische Details. Ergänzend geben einige wenige „Tools“ weitere Hilfestellung, vor allem mit Hinweisen für eine Sicherheitsleitlinie, zur Klassifikation von Daten und einer einfachen Methode für die Risikoanalyse.

Zur Auswahl von Sicherheitsmaßnahmen stellen drei Dokumente ausgewählte, besonders wichtige Maßnahmen als „best practices“ für das Management, IT-Administratoren und andere Angestellt vor; sie sind in Anhang 0 gezeigt.

Zusammenfassende Bewertung

Die Besonderheit des polnischen Ansatzes liegt in seiner Kürze, leichten Lesbarkeit und damit Zugänglichkeit für nicht mit IT-Sicherheit vertrauten und wenig technisch orientierten Personen. Hinzu kommt die anschauliche Aufbereitung in einfach gehaltenen PDF-Dokumenten und Webseite.

Die „Best Practices“ sind eine gute Sammlung überwiegend leicht umsetzbarer grundlegender Maßnahmen und daher für einen Einstieg in die Cybersicherheit und für kleine Organisationen gut geeignet, gleiches gilt für das stark vereinfachte Vorgehensmodell. Sie können durchaus als Vorbild dienen, wie idealerweise aus einem komplexeren und für große Organisationen skalierbaren Ansatz eine Teilmenge als anschauliches und vereinfachtes Material ableitbar sein sollte.

Inhaltlich bringen sie aber keine neuen Erkenntnisse bezogen auf die Aufgabenstellung dieser Arbeit.

4.9 USA: NIST Cybersecurity Framework

4.9.1 Überblick

Das NIST Cybersecurity Framework [22], oft abgekürzt als CSF versteht sich als Leitfaden für Organisationen beliebiger Art und Größe, um Risiken für die Cybersicherheit zu steuern. Es stellt dafür auf hohem Abstraktionsgrad eine Taxonomie von Anforderungen bereit, eine „taxonomy of high-level cybersecurity outcomes“. Wie bei der ISO/IEC 27001 ist diese ergebnisorientiert, ohne Vorgaben, wie die jeweiligen Anforderungen zu erreichen sind.

Das NIST CSF hat damit eine andere Ausrichtung als ISO/IEC 27001:

- Fokus auf Cybersicherheit – keine vollumfängliche Informationssicherheit
- Positionierung als Teil eines im Unternehmen integrierten Risikomanagements – nicht als vollumfassendes ISMS.

Es ist neben der ISO/IEC 27001 ein weithin akzeptierter internationaler Standard, genauso generisch und breit anwendbar. Auch in Form und Umfang ist er ähnlich gehalten, mit einem sehr kompakten Dokument von nur 32 Seiten, das alle relevanten Themen in voller Breite, aber geringer Tiefe nennt.

Die inhaltliche Gliederung ist jedoch vollständig anders und nicht direkt vergleichbar.

Das NIST CSF hat sich aus einem 2014 herausgegebenen und für den Schutz kritischer Infrastruktur veröffentlichten Ansatz entwickelt; die Vorgängerversion 1.1 hieß noch bis Anfang 2024 „Framework for Improving Critical Infrastructure Cybersecurity“. Es ist ein eigenständiger Standard ohne Bezüge z. B. zur ISO/IEC 27001 und es sind keine Zertifizierungen auf seiner Grundlage möglich.

4.9.2 Inhaltliche Beschreibung

Struktur

Das NIST CSF hat drei wesentliche Bestandteile:

Der **CSF Core** ist die erwähnte Taxonomie von für angemessene Cybersicherheit zu erfüllenden Anforderungen, in ihrer Rolle vergleichbar mit den Controls aus dem Anhang A der ISO/IEC 27001. Er hat eine in Inhalt und Form andere Gliederung:

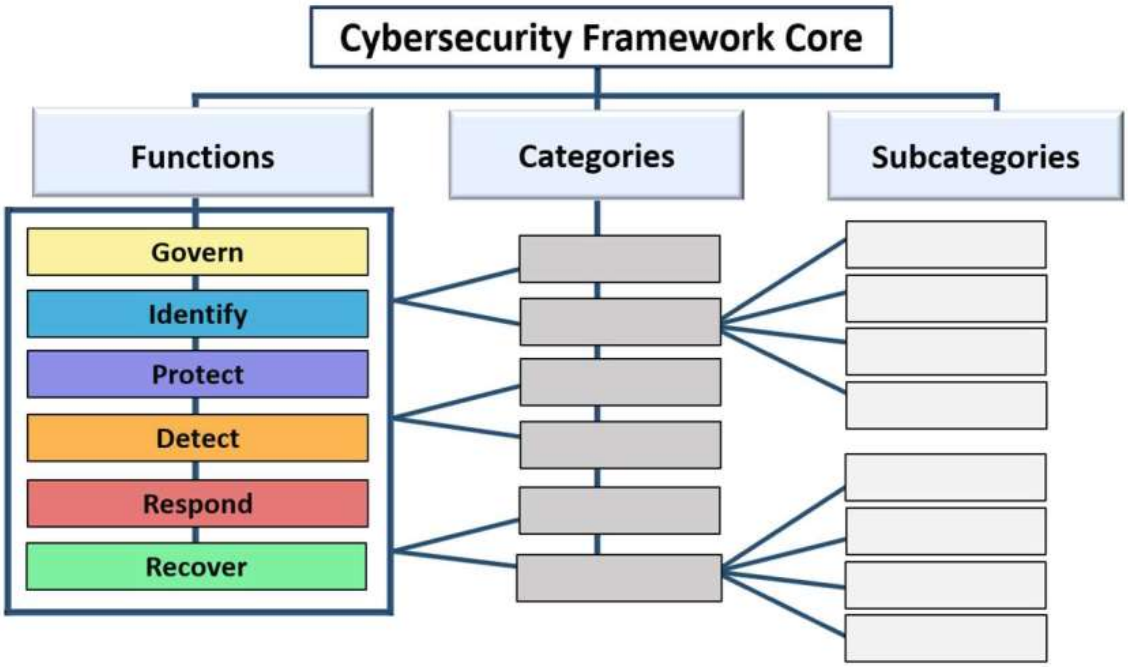


Abbildung 19: NIST CSF Core
Quelle: [22, S. 3]

Die sog. Functions geben eine klare Gliederung aller Anforderungen in wenige Bereiche vor, anders als in der ISO/IEC 27001 jedoch nicht nach ihrem Anwendungsbereich Organisation, Personal, Technik, Physische Sicherheit, sondern nach ihrer Funktion oder Aufgabe im Umgang mit Risiken:

- **Govern;** alle übergeordneten Steuerungsfunktionen wie z. B. Unterstützung der Unternehmensleitung, Festlegung der Strategie zum Risikomanagement, Zuweisung von Rollen und Verantwortlichkeiten, Festschreibung einer „Cybersecurity Policy“.
  Diese Funktion ist im NIST CSF 2.0 Anfang 2024 neu eingeführt worden und eine Annäherung an die ISO/IEC 27001, da sie deutliche Überschneidungen

mit den ISMS-Anforderungen in Kap. 4 – 10 der ISO/IEC 27001 hat, wie schon die beispielhaft genannten Inhalte erkennen lassen.

- **Identify:** alle zum Verstehen der aktuellen Cyberrisiken erforderlichen Aspekte, insbesondere das Asset Management und die Risikobewertung einschließlich der Betrachtung von Schwachstellen und Bedrohungen.
- **Protect:** alle Anforderungen zur Verringerung der Wahrscheinlichkeit und möglichen Auswirkungen von Cyberrisiken. Hier sind die typischen Schutzmaßnahmen wie Authentifizierung, Schulung, Systemhärtung etc. einzuordnen.
- **Detect:** Anforderungen zur Entdeckung von Cyberattacken und Kompromittierungen.
- **Respond:** Anforderungen zur Reaktion auf Sicherheitsvorfälle
- **Recover:** Anforderungen, um von einem Sicherheitsvorfall betroffene Ressourcen und Prozesse wiederherzustellen.

Diese übergeordneten Funktionen sind eine vielzitierte Gliederung, oft in einer Kreisform wie im CSF dargestellt und seit der Anfang 2024 aktuellen Version 2.0 mit der zusätzlichen querschnittlichen Steuerungsfunktion Govern als eigenem Ring:

Abbildung 20: Funktionen des NIST CSF Core
Quelle: [22, S. 5]

Die darunterliegenden Categories und Subcategories sind eine einfache zweistufige hierarchische Gliederung. Ihr Umfang ist mit insgesamt 22 Categories und 106 Subcategories sehr ähnlich den 93 Controls im Anhang A der ISO/IEC 27001.

CSF Profiles sind das zweite Kernelement; sie beschreiben einen Zielzustand und/oder aktuellen Zustand der Organisation hinsichtlich aller Anforderungen des CSF Core, d. h. welche Anforderungen wie umgesetzt werden sollen. Das beinhaltet, die sehr allgemein gehaltenen Anforderungen mit Blick auf die eigene Organisation zu konkretisieren, zu bewerten und zu priorisieren [22, S. 6].

Eine Organisation kann beliebig viele Profile entwickeln, beispielsweise für bestimmte Unternehmensbereiche, eingesetzte Technologien oder gegen ausgewählte Bedrohungen – ein wesentlicher Aspekt, um die Komplexität zu reduzieren. Aus jedem Profil ergeben sich umzusetzende konkrete Maßnahmen.

Für die Erstellung eigener Profile stellt das NIST ein Excel-Template [51] bereit und veröffentlicht beispielhafte Profile als Umsetzungshilfe und Orientierung.

CSF Tiers sind ein dem Reifegradmodell von Prozessen entsprechendes Konzept für den Grad der Gründlichkeit und Detailliertheit, mit dem einzelne Anforderungen umgesetzt sind, laut CSF beschreiben sie „rigor“, die „Rigorosität“ der Umsetzung. Anhang B des CSF 2.0 erklärt die dafür verwendeten vier Stufen, zusammengefasst bedeuten sie:

- **Partial:** die Anwendung von Maßnahmen geschieht ad hoc, nicht systematisch und basierend auf bewusst gesetzten Zielen
- **Risk informed:** Sicherheitsmaßnahmen sind definiert und von der Organisationsleitung bestätigt, aber nicht organisationsweit umgesetzt
- **Repeatable:** Risikobasierte Maßnahmen und Prozesse sind definiert, umgesetzt und werden laufend beobachtet
- **Adaptive:** Risikomanagement für Cybersicherheit ist Teil der Unternehmenskultur.

Beteiligte Dokumente

Das Schlüsseldokument des NIST CSF ist die erwähnte kompakte, der ISO/IEC 27001 vergleichbare Beschreibung des NIST CSF 2.0.

Zur Auslegung der sehr generisch beschriebenen Anforderungen gibt es kein direkt zu diesem Standard gehörendes und der ISO/IEC 27002 vergleichbares Dokument.

Es gibt aber Hinweise als sog. „implementation examples“, die zu jeder Subcategory erläuternde Beispiele zeigen [52].

Zusätzlich verweist das NIST CSF mit sog. „informative references“ auf mehrere andere Publikationen, von denen die im folgenden Abschnitt 4.10 beschriebene Sammlung NIST SP 800-53 die wichtigste ist [52]. Ein Auswerten der zahlreichen Verweise ergibt folgendes Bild:

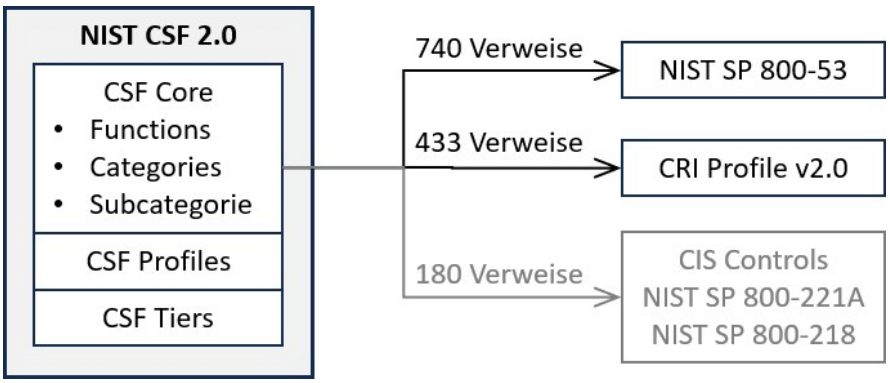


Abbildung 21: Struktur des NIST CSF 2.0 und relevante Dokumente
Quelle: Eigene Darstellung

- 740 Verweise zu NIST SP 800-53; dabei können die Inhalte der NIST SP 800-53 aufgrund ihrer eigenständigen Gliederung inhaltlich leicht abweichen und sind ebenfalls sehr generisch formuliert
- 433 Verweise zu „CRI Profile v2.0“ [53]; diese sind vorrangig an die Finanzbranche gerichtet, aber wegen ihres sehr direkten Zusammenhangs mit den NIST CSF Subcategories leichter umsetzbar. Sie sind eine Publikation des unabhängigen Cyber Risk Institutes, die gezielt zu jeder Subcategory eine oder mehrere konkretisierende Vorschläge nennt.
- eine untergeordnete Zahl von Verweisen zu anderen Publikationen:
  - 85 zu NIST SP 800-221A zur Integration in organisationsweites Risikomanagement
  - 60 zu CIS Controls (in dieser Arbeit nicht behandelt)
  - 35 zu NIST SP 800-218 Secure Software Development.

Ein zusätzliches Online-Tool erlaubt Filtern, Navigieren in und Herunterladen von den Inhalten und Verweisen, ist inhaltlich aber deckungsgleich.

Vorgehensmodell

Das NIST CSF hat kein festes Vorgehensmodell. Dies ist in der bewusst zugunsten einer maximalen Flexibilität und breiten Anwendbarkeit gewählten ergebnisorientierten („outcome based“) Formulierung begründet sowie der angenommenen Einbettung in ein breiter angelegtes Risikomanagement. So wie zu einzelnen Anforderungen bewusst keine Vorgaben existieren, wie sie für die jeweilige Organisation geeignet zu erreichen sind, ist konsequenterweise auch in der insgesamt zu beschreitenden Vorgehensweise keine konkrete Methodik vorgegeben.

Für Umsetzungshinweise verweist das CSF 2.0 auf kommende ergänzende Veröffentlichungen [22, S. iv] und eine gewisse Empfehlung für eine Vorgehensweise ergibt sich aus den **CSF Profiles** und ihrer im CSF gezeigten möglichen Anwendung:

Abbildung 22: Mögliche Schritte zur Anwendung von CSF Profiles
Quelle: [22, S. 6]

In den hier gezeigten Schritten finden sich die Hauptelemente der risikobasierten Auswahl von Sicherheitsmaßnahmen unter Berücksichtigung vorhandener Kataloge wie bei ISO/IEC 27001 wieder, naturgemäß ohne den „Überbau“ eines ISMS:

1. **Scope** – Legt den Umfang eines Profils fest, vergleichbar mit dem Anwendungsbereich eines ISMS oder Geltungsbereich einer Sicherheitskonzeption in der Terminologie des deutschen IT-Grundschutzes.

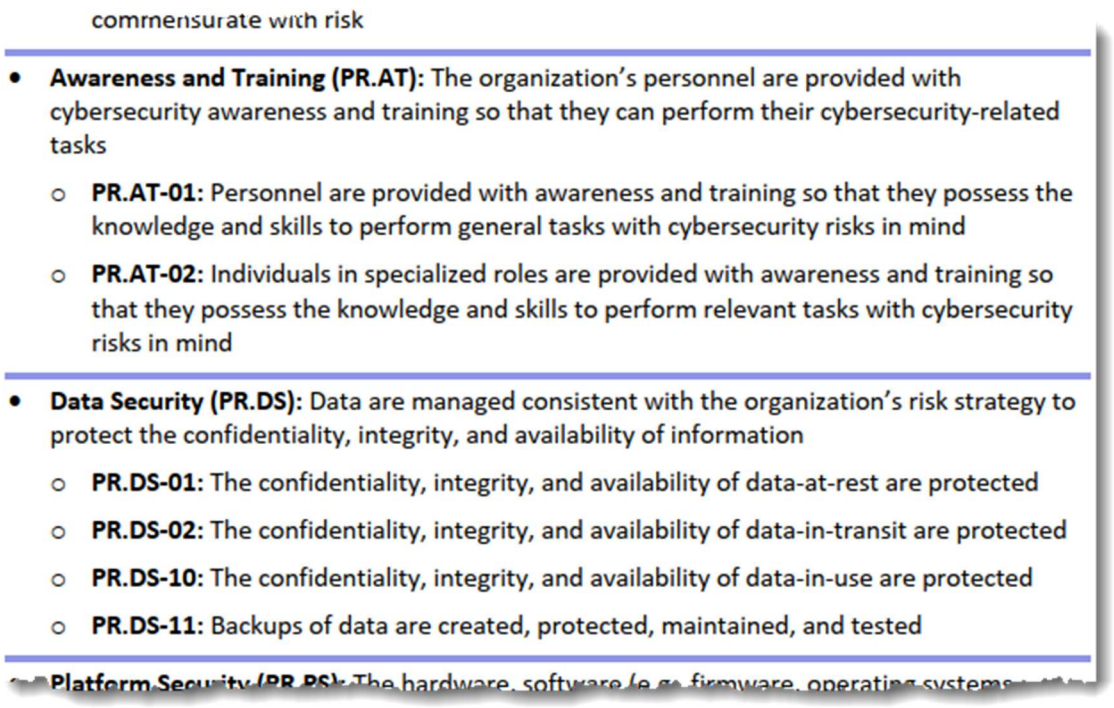
2. **Gather information** – Stellt die Rahmenbedingungen für die Auswahl von Maßnahmen zusammen wie Sicherheitsziele und -richtlinien der Organisation, Vorgehensweise zum Risikomanagement; dies entspricht wichtigen Elementen der ISO/IEC 27001 Kapitel 5 und 6.
3. **Create Profile** – Enthält die eigentliche risikobasierte Auswahl von Maßnahmen bzw. für die Organisation angemessene Ausgestaltung der jeweiligen Subcategories, analog zur Erstellung des „Statement of Applicability“ der ISO/IEC 27001.
4. **Gap analysis** – Ist ein Abgleich von Ist- und Sollzustand zum Ableiten umzusetzender Maßnahmen – ebenfalls Bestandteil der ISO/IEC 27001.
5. **Implementation** – Setzt die definierten Maßnahmen um, wie in der der Implementierungsphase eines ISMS enthalten.

Eine als „Implementation Guidance“, also Umsetzungshilfe bezeichnete Publikation existiert von der ebenfalls öffentlichen amerikanischen Institution Cybersecurity & Infrastructure Security Agency CISA; sie beschreibt ein genau zu diesen Schritten analoges Vorgehen [54].

Sicherheitsmaßnahmen

Die Sicherheitsmaßnahmen im NIST CSF sind die bereits beschriebenen Functions, Categories und Subcategories, formuliert in Form zu erreichender Ergebnisse („outcomes“).

Einen Eindruck von dem sehr hohen Abstraktionsgrad und der Gliederung der Maßnahmen gibt der folgende kleine Ausschnitt zweier Categories mit zugehörigen Subcategories aus der Function „Protect“:


commensurate with risk

- **Awareness and Training (PR.AT):** The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks
  - **PR.AT-01:** Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind
  - **PR.AT-02:** Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind
- **Data Security (PR.DS):** Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information
  - **PR.DS-01:** The confidentiality, integrity, and availability of data-at-rest are protected
  - **PR.DS-02:** The confidentiality, integrity, and availability of data-in-transit are protected
  - **PR.DS-10:** The confidentiality, integrity, and availability of data-in-use are protected
  - **PR.DS-11:** Backups of data are created, protected, maintained, and tested

Platform Security (PR.PS): The hardware, software (e.g., firmware, operating systems

Abbildung 23: Beispielhafter Ausschnitt aus dem CSF Core
Quelle: [22, S. 20]

Ein Abgleich mit den Controls der ISO/IEC 27001 ist aufgrund der vollständig unterschiedlichen Gliederung nicht sinnvoll durchführbar und verspricht auch keine lohnenden Erkenntnisse. Keiner der beiden Standards enthält Themen, die im anderen gar nicht enthalten sind und nicht durch den unterschiedlichen Fokus auf Cybersicherheit bzw. ISMS für Informationssicherheit bedingt sind.

4.9.3 Zusammenfassende Bewertung

Das NIST CSF ist ein in Form und Vorgehensweise der ISO/IEC 27001 vergleichbarer Standard mit unterschiedlicher Zielsetzung und Schwerpunkt sowie ebenfalls breiter internationaler Akzeptanz.

Wesentliche Gemeinsamkeiten sind:

- Vergleichbarer Umfang der sehr kompakten Kerndokumente
- Vergleichbar hoher Abstraktionsgrad
- Orientierung an ergebnisorientierter Beschreibung von Anforderungen für größtmögliche Flexibilität und breite Anwendbarkeit
- Vergleichbare Zielsetzung der ganzheitlichen Verankerung von Cybersicherheit bzw. Informationssicherheit in der gesamten Organisation

- Entsprechend vergleichbare übergreifende Anforderungen zur Steuerung der Cyber- bzw. Informationssicherheit in Form der Function „Govern“ im NIST CSF bzw. der ISMS-Anforderungen in der ISO/IEC 27001
- Risikobasierte Auswahl und Ausgestaltung von Sicherheitsmaßnahmen.

Wesentliche Unterschiede sind:

- Der Fokus auf Cybersicherheit als Teil eines unternehmensweiten Risikomanagements bei NIST vs. Informationssicherheit umgesetzt durch ein ISMS bei ISO/IEC 27001
- Der Ansatz der „Tiers“ im NIST CSF für unterschiedliche Gründlichkeit der Umsetzung von Anforderungen findet sich in ISO/IEC 27001 nicht wieder.
- Sehr zahlreiche Verweise des NIST CSF auf wiederum sehr umfangreiche Controls ergeben einen deutlich höheren Umfang als bei der ISO/IEC 27002.
- Gliederung von Sicherheitsmaßnahmen nach Anwendungsbereich in der ISO/IEC 27001 und nach Schutzfunktionen im NIST CSF.

Die anders geartete Gliederung anhand der Schutzfunktionen Identify – Protect – Detect – Respond – Recover erscheint sinnvoller, da sie Sicherheitsaspekte und damit das eigentliche Wesen der „Controls“ in den Vordergrund rückt.

Kritisch zu sehen ist der zu erwartende hohe Implementierungsaufwand des NIST CSF, da die zahlreichen Verweise zur Ausgestaltung des CSF Core überwiegend in die umfangreichen, ebenfalls sehr generisch formulierten und auslegungsbedürftigen Controls der NIST SP 800-53 verweisen. Zudem ist eine so hohe Zahl von Querverweisen zwischen sehr unterschiedlichen Dokumenten eine praktische Herausforderung. Hier ist ein Bedarf an konkretisierenden Umsetzungshilfen offensichtlich.

Die empfohlene Anwendung eines Excel-Templates zur Erstellung von CSF Profiles erscheint nicht praktikabel, siehe Anhang 0 zur Veranschaulichung. Eine leichter handhabbare Umsetzung der an sich einleuchtenden und schlüssigen Vorgehensweise darin wäre wünschenswert.

Auch ist die Unterstützung durch veröffentlichte wiederverwendbare Profile nur gering; für die noch neue Version 2.0 des CSF sind erst zwei veröffentlicht, aber auch für die 10 Jahre existierende Vorgängerversion 1.1 nur 15 recht spezialisierte [55].

Positiv zu werten ist der Ansatz der Tiers, da unterschiedliche Grade der Umsetzungstiefe bei den sehr generisch formulierten Anforderungen sinnvoll ist, um unterschiedlichen Organisationen gerecht zu werden.

4.10 USA: NIST SP 800-53

4.10.1 Überblick

Ziel der „Special Publication“ 800-53 des US-amerikanischen NIST [20] ist, einen umfassenden Katalog von als „controls“ bezeichneten Maßnahmen für Sicherheit und Datenschutz von informationsverarbeitenden Systemen und Organisationen bereitzustellen [20, S. ii]. Sie sind zur Umsetzung als Teil eines organisationsweiten Risikomanagements erstellt, für das ein separater Standard NIST SP 800-37 existiert.

Sie ist eine komplexe Sammlung von Maßnahmen zur Informationssicherheit, die neben dem Grundschutz-Kompendium umfangreichste verfügbare auf knapp 500 Seiten. Die meisten Maßnahmen sind generisch, ohne Bezug zu konkreten IT-Systemen und brauchen daher für eine konkrete Anwendung Interpretation und Auslegung für den jeweiligen Kontext. Das macht sie sehr universell – zur Anwendung auf beliebige informationsverarbeitende Systeme und Organisationen, zum Schutz beliebiger Zielobjekte, Prozesse, Systeme, Personen und gegen vielfältige Bedrohungen. Wegen ihrer Gliederung und ihres hohen Abstraktionsgrades ist sie grundlegend anders als das Grundschutz-Kompendium.

4.10.2 Inhaltliche Beschreibung

Sicherheitsmaßnahmen

Es handelt sich bei NIST SP 800-53 um eine reine Sammlung von „Controls“, wobei der Begriff Control hier als Schutzmaßnahme zum Erreichen von Sicherheitszielen definiert ist [20, S. 8], nicht wie im ISO/IEC 27001-Standard über ihre Auswirkung auf Risiken.

Die Controls sind gegliedert in 20 nachfolgend gezeigte „**control families**“:

ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

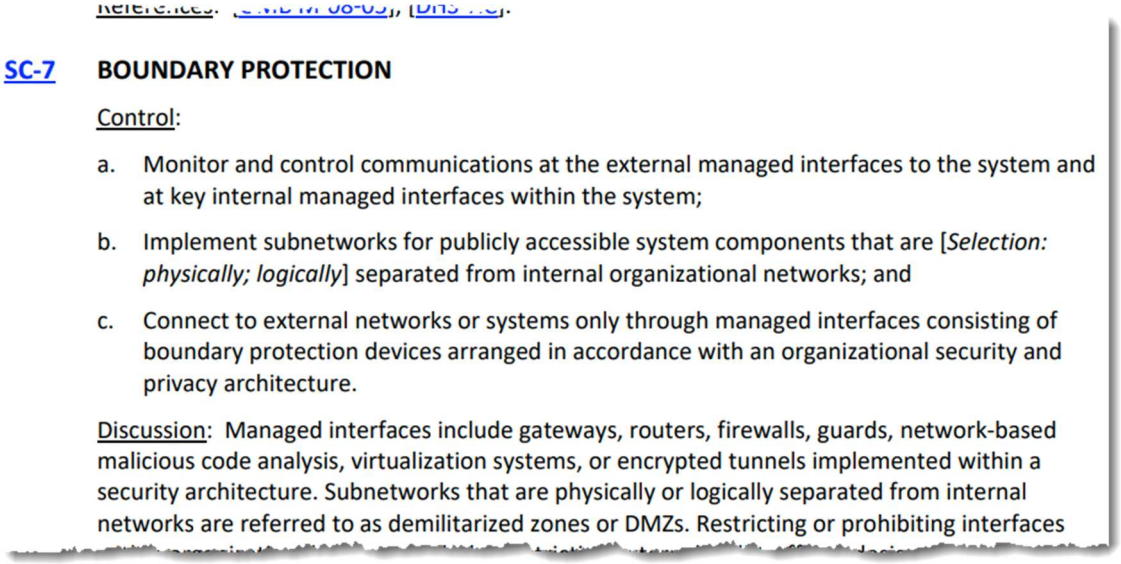
Abbildung 24: 20 Control Families der NIST SP 800-53
Quelle: [20, S. 8]

Innerhalb jeder Familie sind alle zugehörigen Controls mit einer laufenden Nummerierung aufgeführt und mitunter durch sog. „Control Enhancements“ ergänzt, die zusätzliche Funktionalität hinzufügen, höhere Wirksamkeit erzielen können oder spezielle Ausprägungen formulieren. Die Sammlung besteht aus insgesamt

- knapp 1200 Einträgen, darunter
- 322 Controls und
- 867 Control Enhancements.

Die Controls sind auf hohem Abstraktionsniveau formuliert, oft nur mit Bezug auf das jeweilige „system“; die Anwendbarkeit für verschiedene Systemarten wie Server, Netzwerke, Clients etc. ist damit bewusst offengelassen und in jedem Anwendungsfall zu bewerten: „Controls can be implemented within any organization or system that processes, stores, or transmits information.“ [20, S. 2].

Hier ein veranschaulichendes Beispiel:



SC-7 BOUNDARY PROTECTION

Control:

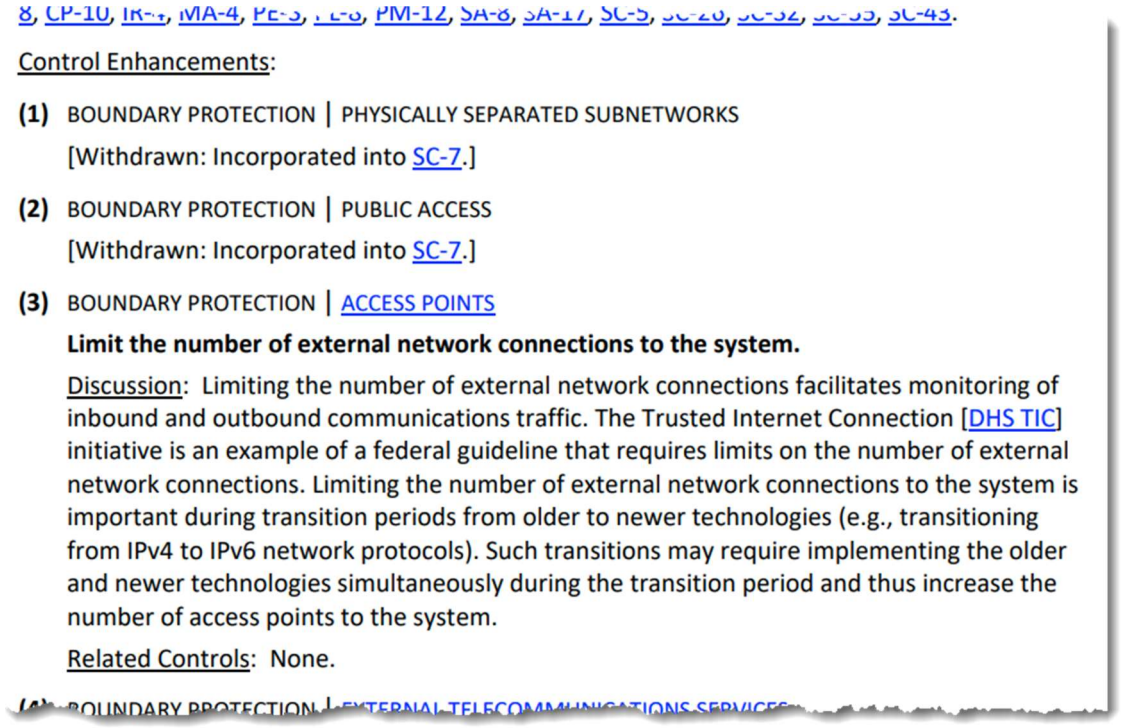
a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;

b. Implement subnetworks for publicly accessible system components that are [*Selection: physically; logically*] separated from internal organizational networks; and

c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

Discussion: Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code analysis, virtualization systems, or encrypted tunnels implemented within a security architecture. Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces

Abbildung 25: Beispiel einer Control aus NIST SP 800-53
Quelle: [20, S. 297]



Control Enhancements:

(1) BOUNDARY PROTECTION | PHYSICALLY SEPARATED SUBNETWORKS

[Withdrawn: Incorporated into SC-7.]

(2) BOUNDARY PROTECTION | PUBLIC ACCESS

[Withdrawn: Incorporated into SC-7.]

(3) BOUNDARY PROTECTION | ACCESS POINTS

Limit the number of external network connections to the system.

Discussion: Limiting the number of external network connections facilitates monitoring of inbound and outbound communications traffic. The Trusted Internet Connection [DHS TIC] initiative is an example of a federal guideline that requires limits on the number of external network connections. Limiting the number of external network connections to the system is important during transition periods from older to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols). Such transitions may require implementing the older and newer technologies simultaneously during the transition period and thus increase the number of access points to the system.

Related Controls: None.

Abbildung 26: Beispiel einer Controls Enhancement aus NIST SP 800-53
Quelle: [20, S. 298]

Eine Besonderheit in der Formulierung der Controls macht sie gewöhnungsbedürftig zu lesen: Die Maßnahmen enthalten an vielen Stellen Angaben in eckigen Klammern, die kontextabhängig mit unterschiedlichen Parametern zu ersetzen sind.

Dafür ein Beispiel zum Thema Access Control, zitiert aus NIST SP 800-53:

> **AC-1 Policy and Procedures**
>
> Control:
>
> a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
>
> 1. [Selection (one or more): Organization-level; Mission/business process-level; Systemlevel] access control policy that:
>
> …

Hier ist „[Assignment: organization-defined personnel or roles]“ bei konkreter Anwendung mit der in der Organisation verwendeten Rollenbezeichnung zu ersetzen. Entsprechend ist „[Selection (one or more): Organization-level; Mission/business process-level; Systemlevel]“ mit einem der vorgeschlagenen Werte wie z. B. organization-level zu ersetzen.

Das ist ein weiteres Merkmal für maximale Flexibilität, erschwert aber den Einstieg und die Arbeit mit dem Dokument, da die ohnehin anspruchsvoll formulierten Controls nicht in einer auf Anhieb flüssig lesbaren Form vorliegen.

Vorgehensweise

Die NIST SP 800-53 ist eine Sammlung von Controls, ohne Angabe von Prioritäten, ohne ein zugehöriges Vorgehensmodell – bewusst „separating control selection processes from the controls“.

Eine gewisse Orientierung bei der Auswahl von Controls ergibt sich aus zwei ergänzenden Dokumenten:

- **Kategorisierung** von IT-Systemen – Ein anderer Standard der NIST, bezeichnet als FIPS 199 [56] definiert „Security Categorizations“ für staatliche IT-Systeme. Dies sind Kategorien der Schutzbedürftigkeit; die Bewertung erfolgt anhand erwarteter negativer Auswirkungen:
  - „low“ für begrenzte („limited adverse effect“)
  - „medium“ für signifikante („serious adverse effect“)
  - „high“ für schwerwiegende oder katastrophale („severe or catastrophic adverse effect“).

Dabei sind die Auswirkungen separat für Vertraulichkeit, Verfügbarkeit und Integrität zu betrachten und die höchste gefundene Einstufung ist für alle Schutzziele anzuwenden.

- **Mindestanforderungen je Kategorie** – NIST SP 800-53B [57] definiert „Control Baselines" = Sätze von ausgewählten Controls für die zuvor definierten Stufen von Schutzbedarf.
  Aus den insgesamt 1189 controls und control enhancements sind
  - 149 empfohlen für die Einstufung low
  - 287 für die Einstufung medium
  - 370 für die Einstufung high.

  Die übrigen sind ohne Empfehlung und fast alle im Ermessen der jeweiligen Organisation anzuwenden; ein kleiner Teil von 21 bzw. 37 Maßnahmen ist explizit ausgeschlossen oder nur auf Unternehmensebene umzusetzen.

4.10.3 Zusammenfassende Bewertung

Die Publikation NIST SP 800-53 hat eine Sonderrolle. Sie ist kein ganzheitlicher Ansatz für IT-Sicherheit in Organisationen im Sinne der Aufgabenstellung, aber als die umfangreichste und vollständigste verfügbare Sammlung von Sicherheitsmaßnahmen ein wertvolles Grundlagendokument und relevant, da andere hier betrachtete Ansätze sich auf sie beziehen, insbesondere das wichtige NIST CSF.

Zwei Aspekte scheinen nachahmenswert für andere Ansätze

- Die ergebnisorientierte Formulierung („outcome based"), wie sie auch das NIST CSF und nicht ganz so konsequent ISO/IEC 27001 verwenden, sorgt für größtmögliche Flexibilität und Anwendbarkeit.
- Die inhaltliche Gliederung und Betonung der jeweiligen Schutzfunktion ist methodisch konsequent und vorbildlich für ganzheitliche Ansätze zur IT-Sicherheit, da sie das Hauptanliegen – die Sicherheit – betont.

Ohne zusätzliche Umsetzungshilfen ist NIST SP 800-53 schwer handzuhaben und sehr aufwändig. Die zahlreichen Einschübe für beabsichtigte indivduelle Anpassungen machen die Publikation gewöhnungsbedürftig und für Einsteiger schwer zu lesen. Zudem ist der Aufwand für eine konkrete Auslegung bezogen

auf einen speziellen Anwendungsfall sehr hoch. Als Referenz bei der Erstellung von ganzheitlichen Ansätzen wie dem IT-Grundschutz, die daraus konkretere Maßnahmen ableiten, ist diese Sammlung jedoch sehr wertvoll.

Sie kann mit ihrer Gliederung aller Maßnahmen eine gute Orientierung sein, um Vorgabedokumente thematisch zu strukturieren. Jede Familie von Controls beginnt mit einer Maßnahme, zu dem jeweiligen Thema eine Richtlinie („policy“) zu erstellen. Diese Struktur in der Praxis zu testen, erscheint naheliegend und aufgrund fehlender konkreter Vorschläge zur Strukturierung von Vorgabedokumenten in anderen Ansätzen reizvoll, würde aber den Rahmen dieser Arbeit übersteigen.

Da sie bei den meisten Controls bewusst offenlässt, für welche Systeme sie anwendbar sind, wäre eine Umsetzungshilfe wünschenswert, die genau diese Information liefert und Controls systembezogen präzisiert – was zu einem den Bausteinen des Grundschutz-Kompendiums ähnlichen Ansatz führen würde.

Wünschenswert wäre eine klarere risikobasierte Angabe von Prioritäten. Eine Studie von MITRE [58, S. 3] zeigt, dass dadurch eine sehr stark begrenzte Auswahl von Maßnahmen möglich sein kann: Nur 10 (!) Controls konnten Abhilfe gegen Techniken schaffen, die 90 % von in der Realität beobachteten Angriffen ausmachen; basierend auf einer großen Datenbasis von 6 Mio. Beobachtungen im Zeitraum von 2019 – 2021.

4.11 ISO/IEC-Standards und Cybersicherheit

4.11.1 ISO/IEC 27100-Reihe

In dieser Reihe schlagen die ISO/IEC-Publikationen eine Brücke zur Cybersicherheit und erläutern deren Zusammenhang mit ISMS und Informationssicherheit, die wichtigsten Dokumente sind:

- ISO/IEC **TS 27100 Cybersecurity – Overview and concepts** [12]
  Dieses Dokument enthält analog zu ISO/IEC 27000 Definitionen und erläutert die Beziehung zwischen ISMS und Cybersecurity (ebd. Kap. 5.2):

- Cyberrisiken (s. 3.1) sind als eine besondere Art von Risiken ein Input für den risikobasierten Ansatz eines ISMS.
- Umgekehrt ist ein ISMS ein bewährter und systematischer Weg, auch Cyberrisiken zu steuern.

- ISO/IEC **TR 27103 Cybersecurity and ISO/IEC and IEC Standards** [59]
  Dieser Technical Report beschreibt die Beziehung eines ISMS nach ISO/IEC 27001 zu Cybersicherheit und bestätigt die gerade genannten Punkte: „An ISMS as described in ISO/IEC 27001 is a well proven way for any organization to implement a risk-based approach to cybersecurity“ (ebd. S. v). Ferner schlägt er eine Brücke zum zuvor diskutierten NIST Cybersecurity Framework (s. 4.9):
  - Er betont die Notwendigkeit eines risikobasierten Ansatzes, was auch Kern des NIST CSF ist.
  - Er beschreibt Funktionen, die ein Cybersecurity Framework haben soll und übernimmt dafür exakt die des NIST CSF v1.1.
  - Auch die weiteren Bestandteile des NIST CSF Core – Categories und Subcategories – werden identisch als mögliche Bestandteile eines Cybersecurity Frameworks aufgelistet und entsprechenden Controls aus ISO/IEC 27001 und 27002 zugeordnet.
- ISO/IEC **TS 27110 Cybersecurity framework development guidelines** [60]
  Mit dieser Veröffentlichung definiert die ISO/IEC einen Rahmen für die Entwicklung von Cybersecurity Frameworks – wiederum in genauer Übereinstimmung mit dem NIST CSF. Dabei nennt sie die fünf Funktionen des NIST CSF als notwendige Bestandteile und die untergeordneten Categories und Subcategories als mögliche „Beispiele“.
  In der Einleitung betont die ISO/IEC 27110, dass es nicht beabsichtigt ist, die Anforderungen eines ISMS nach ISO/IEC 27001 abzulösen oder zu ersetzen (ebd. S. v).

Insgesamt etabliert die ISO damit eine Koexistenz der beiden etablierten Standards ISO/IEC 27001 und dem NIST Cybersecurity Framework. Das NIST CSF wird zwar an keiner Stelle explizit erwähnt, aber die Kompatibilität zu ISO/IEC 27001 dokumentiert. Zudem lässt die ISO sinnvollen Raum für weitere

Standards und insbesondere detailliertere Umsetzungshilfen, wirkt aber daraufhin, dass diese möglichst in der vom NIST CSF vorgegebenen Struktur bleiben.

Diese Publikationen ergeben nur Sinn, wenn ISO keinen eigenen Standard für Cybersicherheit herausgibt, eine „ISO/IEC 27001 für Cybersicherheit“ ist demnach *nicht* zu erwarten.

4.11.2 ISO/IEC 27032 zu Internetsicherheit

Die ISO/IEC 27032 [16] schlägt ebenfalls eine Brücke zur Internetsicherheit und damit einem wesentlichen Teil der Cybersicherheit, ist aber als Erweiterung zu ISO/IEC 27001 und 27002 zu sehen.

Bezüglich der ISMS-Anforderungen in Kap. 4 – 10 der ISO/IEC 27001 ergänzt sie entsprechende Inhalte für die „interested parties“ und für die Risikoanalyse in Form von Bedrohungen und möglichen Schwachstellen.

Für die in ISO/IEC 27002 erläuterten Controls ergänzt sie diverse für das Internet spezifische Aspekte und ordnet sie konkreten Controls zu. Der Abstraktionsgrad ist ähnlich hoch wie in der ISO/IEC 27002, so dass ebenfalls eine Ausgestaltung der Anforderungen erforderlich ist.

In einer vollständigen Umsetzung der ISO/IEC 27001, die zeitgemäß Cyberrisiken berücksichtigt, sollte die ISO/IEC 27032 eingearbeitet werden, auch wenn sie in ISO/IEC 27001 und 27002 nicht referenziert ist.

4.12 BSI und Cybersicherheit

Da die meisten folgenden, zum Vergleich herangezogenen Ansätze Cybersicherheit in den Mittelpunkt rücken, ist ein genauerer Blick angebracht, welche Rolle diese im IT-Grundschutz und beim BSI spielt.

Im IT-Grundschutz gibt es speziell für Cybersicherheit lediglich einen Verweis auf einen „Cyber-Sicherheits-Check“, den das BSI in Kooperation mit der ISACA herausgibt. Dieser spielt nur eine nachgelagerte Rolle, die IT-Grundschutz-

Methodik erwähnt ihn ganz am Ende im Zusammenhang mit der Überprüfung der Umsetzung von Sicherheitsmaßnahmen [29, S. 168].

Die Bedeutung der Cybersicherheit steht außer Frage, auch das BSI betont sie z. B. in seinem jährlichen Lagebericht [37]. Die zugehörigen Aktivitäten und Veröffentlichungen sind jedoch separat vom IT-Grundschutz:

- Es gibt eine im Organigramm des BSI erkennbare organisatorische Trennung [61]:
  - Der IT-Grundschutz ist zusammen mit anderen BSI-Standards einem Referat in der Abteilung für „Standardisierung, Zertifizierung und Sicherheit von Telekommunikationsnetzen“ zugewiesen
  - Daneben gibt es drei andere mit Cybersicherheit befasste Abteilungen, darunter eine „Cybersicherheit für Wirtschaft und Gesellschaft“, mit dem für die „Allianz für Cybersicherheit“ zuständigen Referat.
- Die nach außen gerichteten Aktivitäten und Veröffentlichungen zur Cybersicherheit sind in der Allianz für Cyber-Sicherheit gebündelt [62], die vom IT-Grundschutz unabhängige Veröffentlichungen zur Cybersicherheit herausgibt.

Ein ganzheitlicher Ansatz zur Cybersicherheit – eigenständig oder als Teilmenge des IT-Grundschutzes – existiert nicht; die Allianz für Cybersicherheit hat aber diverse einzelne Veröffentlichungen zu wichtigen Themen publiziert, an einer Stelle auch gesammelte Empfehlungen für Unternehmen [63].

Die dort veröffentlichten Dokumente sind im Anhang 0 aufgelistet, zusammenfassend lässt sich festhalten:

- Sie unterliegen keiner fortlaufenden Aktualisierung; die meisten Veröffentlichungen stammen von 2018 und einzelne von 2012 oder 2022.
- Die Veröffentlichungen sind unabhängig vom IT-Grundschutz. Ein Befolgen der Ratschläge der Allianz für Cyber-Sicherheit und eine Anwendung des IT-Grundschutzes würde zu Redundanzen, Überschneidungen und entsprechendem Mehraufwand führen.

4.13 Belgien: Cyber Fundamentals Framework

4.13.1 Überblick

Das belgische Cyber Fundamentals Framework hat zum Ziel, konkrete Maßnahmen vorzuschlagen, die das Risiko der gängigsten Cyber-Attacken reduzieren [64].

Es ist nach eigenen Angaben basierend auf NIST CSF, ISO/IEC 27001 und 27002 sowie CIS Controls und dem Standard IEC 62443 für industrielle Kommunikationsnetze. In seiner Struktur entspricht es jedoch genau dem NIST CSF 1.1 und ist deshalb als Umsetzungshilfe zum NIST CSF anzusehen.

Es veröffentlicht in überschaubarem Umfang konkrete Empfehlungen für Sicherheitsmaßnahmen in vier Abstufungen. Die Maßnahmen sind gegen vom belgischen CERT beobachtete erfolgreiche Cyberattacken validiert und geben nach Angaben der belgischen Behörde für Cybersicherheit mit ihrem Umfang steigenden Schutz:

- Stufe Basic gegen 82 % der beobachteten Cyberattacken
- Stufe Important gegen 94 %
- Stufe Essential gegen 100 %.

Darunter existiert die vierte Stufe Small, eine gegenüber Basic nochmals erheblich verkleinerte Einstiegsvariante ohne Angabe der geschätzten Schutzwirkung.

4.13.2 Inhaltliche Beschreibung

Der belgische Ansatz ist eine reine Sammlung von Sicherheitsmaßnahmen, enthält keinerlei Hinweise für ein Vorgehensmodell. Die Sicherheitsmaßnahmen übernehmen neben der Struktur des NIST CSF 1.1 auch deren genaue Formulierung von Subcategories einschließlich ihrer IDs. Auf diese Weise sind die beiden Ansätze direkt verknüpft.

Entsprechend der vom belgischen Centre for Cybersecurity ermittelten Prioritäten listen die drei Stufen der Cyber Fundamentals eine mit jeder Stufe wachsende Anzahl von Subcategories des NIST CSF.

Function	NIST CSF 1.1	BASIC	IMPORTANT	ESSENTIAL
Identify	29	10	25	26
Protect	39	15	36	37
Detect	18	4	15	17
Respond	16	3	15	15
Recover	6	1	4	6
gesamt	**108**	**33**	**95**	**101**

Tabelle 5: Anzahl der in den belgischen Cyber Fundamentals abgedeckten Subcategories des NIST CSF 1.1
Quelle: Eigene Auswertung

Neben der reinen Zahl der abgedeckten Sicherheitsmaßnahmen ist die Intensität und Gründlichkeit der Umsetzung zu beachten, wie im NIST CSF in Form der Tiers angelegt. Diese kann im belgischen Ansatz ebenfalls mit jeder Stufe zunehmen; nachfolgend ein Beispiel hierzu, das auch die Art der gegebenen Umsetzungshinweise gut veranschaulicht:

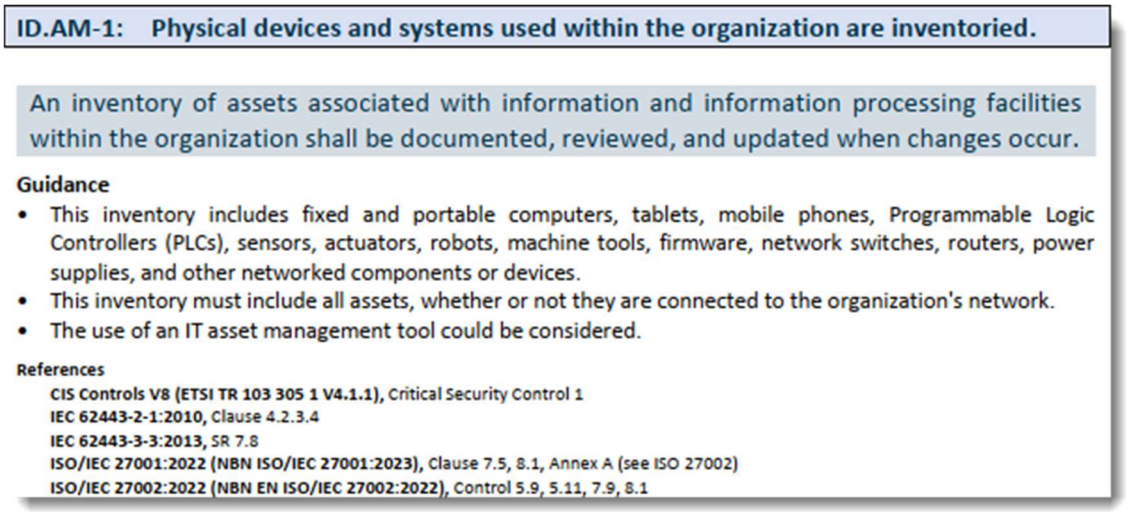


Abbildung 27: Informationen zu Subcategory ID.AM-1 in den belgischen Cyber Fundamentals Basic
Quelle: [65]

Der gezeigte Ausschnitt formuliert nur die generelle Anforderung der Stufe „Basic“, ein Inventar aller Assets von informationsverarbeitenden Geräten vorzuhalten.

In den nächsten Stufen nimmt die Umsetzungstiefe zu:

- Die Stufe „Important“ ergänzt:
  - Das Inventar ist bei Änderungen im Unternehmensumfeld anzupassen und muss bestimmte Angaben für Zuordnung von Verantwortlichkeiten haben.
  - Entdeckte und nicht unterstützte Hardware ist zu isolieren, zu ersetzen zu entfernen.
- Die Stufe „Essential“ ergänzt: Es sollten automatisierte Verfahren zum Entdecken nicht autorisierter Hardware im Netzwerk eingesetzt werden.

Als zusätzlicher Indikator für besonders wichtige Maßnahmen sind einzelne als „key measures“ herausgehoben.

Die vierte Publikation „Cyber Fundamentals Small“ [66] ist als Einstieg und für „micro organizations“ gedacht und auf einen minimalen Umfang von nur sieben klaren Maßnahmen reduziert, ohne Bezug zum NIST CSF.

4.13.3 Zusammenfassende Bewertung

Der belgische Ansatz ist nicht nur eine Umsetzungshilfe zum NIST CSF 1.1, sondern auch eine wichtige Orientierung in Form von Prioritäten der Sicherheitsmaßnahmen, der auf in der Realität beobachteten Cyberattacken beruht und somit auf Informationen, die Organisationen normalerweise nicht zugänglich haben – und man sich von offiziellen Stellen als Hilfestellung wünscht. Gleichzeitig ist dies eine konsequente Umsetzung eines risikobasierten Vorgehens, wie ihn alle anderen betrachteten Ansätze auch fordern.

In seinen Umsetzungshinweisen geht er einen sinnvollen Schritt weiter als das sehr generisch formulierte NIST CSF. Die konkrete Umsetzung in einem gegebenen Praxisfall würde immer noch gewissen weiteren Aufwand zur Ausgestaltung für eine bestimmte Organisation bedeuten, aber weniger als das NIST CSF für sich alleine.

4.14 Portugal: National Cybersecurity Framework NCF-PT

4.14.1 Überblick

Das portugiesische National Cybersecurity Framework [67], abgekürzt NCF-PT, versteht sich als nationales Instrument, das Organisationen Maßnahmen für die wichtigsten Herausforderungen bezüglich Cybersicherheit anbietet (ebd., S. 10).

Es ist eine Art Implementierung des NIST CSF 1.1, übernimmt alle seine Subcategories als Sicherheitsmaßnahmen und ergänzt Grundlagen zum Risikomanagement basierend auf ISO/IEC 27005.

4.14.2 Inhaltliche Beschreibung

Das NCF-PT übernimmt alle Subcategories des NIST CSF 1.1 als Sicherheitsmaßnahmen und ergänzt kurze Beschreibungen sowie stichwortartige Umsetzungshinweise. In stichprobenartigen Betrachtungen erscheint der Nutzen dieser Ergänzungen begrenzt, da die Erläuterungen immer noch sehr allgemein gehalten sind und oft nur die Beschreibung des NIST CSF umformulieren oder in sich Wiederholungen zeigen. Zwei Beispiele sind im Anhang 8.18 gezeigt.

Daneben existiert eine weitere, möglicherweise für die Umsetzung des NIST CSF hilfreichere Publikation, die für jede Anforderung des NIST CSF 1.1 Kriterien beschreibt, um den Umsetzungsgrad entsprechend der Tiers im NIST CSF zu bewerten. Sie ist aber nur auf Portugiesisch verfügbar.

Als Vorgehensweise beschreibt das Framework ein generisches Vorgehen zur Risikoanalyse entlang der ISO/IEC 27005, aus ihr ergeben sich keine neuen Erkenntnisse für die vergleichende Betrachtung dieser Arbeit.

4.14.3 Zusammenfassende Bewertung

Das portugiesische Cyber Security Framework bringt keine für die vergleichende Betrachtung relevanten neuen Erkenntnisse.

Hilfreich ist er zweifellos als nationale Umsetzungshilfe, da es alle Inhalte des CSF auf portugiesischer Sprache verfügbar macht.

4.15 Israel: Cyber Defense Doctrine 2.0

4.15.1 Überblick

Ziel der israelischen „Cyber Defense Doctrine 2.0“ [68] ist es, der isrealischen Wirtschaft eine ganzheitliche, systematische und professionelle Methode für das Management von Cyberrisiken anzubieten.

Es ist ein auf dem NIST CSF basierender nationaler Standard, wobei die Beziehung zum amerikanischen Vorbild nur eine recht lose ist. Die Vorgängerversion war die israelische „Cyber Defense Methodology for an Organization 1.0“, erschienen 2017. Sie bezog sich explizit auf das NIST CSF und folgte in seinen Maßnahmen dessen Gliederung in Identify – Protect – Detect – Respond – Recover [69]. Das NIST selber erwähnt die Anwendung ihres CSF in Israel als eine „Success Story“ [70], auch mit Verweis auf die Version 2.0. Die Cyber Defense Doctrine 2.0 selbst schreibt aber nicht mehr vom NIST CSF als Basis, sondern dass die Maßnahmen vom Israel National Cyber Directorate geschrieben seien für ein Framework „ähnlich dem NIST CSF“ [68, S. 41]. Die Gliederung entlang der Funktionen des NIST CSF hat die Version 2.0 nicht mehr und ist auch in den Details der Maßnahmenbeschreibung eigenständig, weshalb abweichend von der Darstellung des NIST der israelische Ansatz als ein eigenständiger zu bewerten ist.

Der israelische Standard hat eine Zweiteilung in ein Dokument zur Methodik und eine Sammlung von „Controls“, wobei für kleine Organisationen eine erhebliche Vereinfachung vorgesehen ist. Für größere Unternehmen erfolgt auch hier eine risikobasierte Auswahl von Maßnahmen, unter Berücksichtigung eines vordefinierten Kataloges von Standard-Maßnahmen. Als eigenes und besonderes Element enthält er eine pragmatische eigene Methode zur Risikoanalyse.

4.15.2 Inhaltliche Beschreibung

Abstufung nach Organisationsgröße

Der israelische Ansatz unterscheidet zwei Kategorien von Unternehmen:

- Category A = Organisationen mit einem zu erwartenden finanziellen Schaden von max. 1,5 Mio. USD aus Cyber-Vorfällen
- Category B = alle anderen Organisationen.

Für die Beurteilung, ob Schaden aus Cyberangriffen die Grenze von 1,5 Mio. USD überschreiten, gibt es keine eindeutigen Kriterien, nur hilfsweise Fragen und einzelne Empfehlungen wie z. B. ab einer Umsatzgrenze von 60 Mio. USD oder in bestimmten Branchen wie Gesundheitswesen, IT oder als akademische Einrichtung sich der Kategorie B zuzuordnen.

Vorgehensweise

Unternehmen der Kategorie A durchlaufen ein abgekürztes Verfahren, das ohne Risikoanalyse direkt ausgewählte Sicherheitsmaßnahmen umsetzt. Für Kategorie B ist ein Vorgehen mit Risikoanalyse und Berücksichtigung eines Katalogs von 120 Sicherheitsmaßnahmen vorgesehen.

Die Vorgehensweise für Kategorie B sind sehr ähnlich zu den bereits vorgestellten Ansätzen:

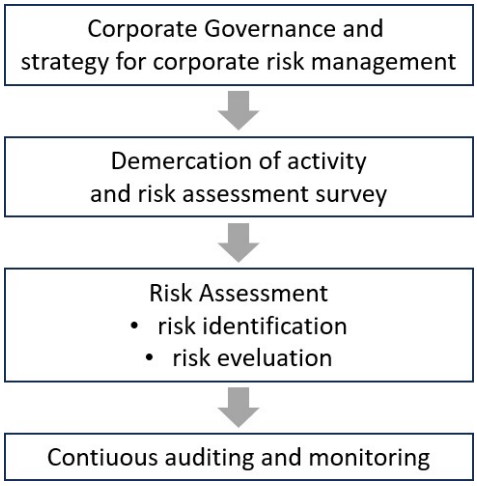


Abbildung 28: Vorgehensweise der israelischen Cyber Defense Doctrine für Categeory B-Unternehmen
Quelle: Eigene Darstellung, basierend auf [68, S. 26 ff.]

Die ersten beiden Stufen entsprechen den typischen Steuerungsaufgaben der Unternehmensleitung – sogar mit einem Hinweis „sometimes called ISMS“ [68, S. 26] – sowie der Festlegung eines Geltungsbereichs.

Ein eigenständiges Modell findet sich in der Risikobewertung zur Einschätzung von potentiellen Auswirkungen und Eintrittswahrscheinlichkeiten, das die übliche Schätzung von Eintrittswahrscheinlichkeiten mit einer pauschalierten Bewertung der Bedrohungslage und Angriffsfläche anhand einfacher Fragen wie der Verbindung mit externen Netzen und der Häufigkeit von Patches ersetzt.

Sicherheitsmaßnahmen

In Kategorie A ist eine kleine Zahl von Maßnahmen umzusetzen, gegliedert in „Ten Commandments“ und im Anhang A mit 25 Maßnahmen detailliert, Details hierzu sind in Anhang 0. Dabei enthalten die Maßnahmen einzelne simple und leicht umzusetzende wie den Einsatz von Schutzprogrammen vor Schadsoftware und das regelmäßige Aktualisieren von Systemen ebenso wie diverse umfangreiche, die nicht ohne Vorwissen anhand der gegebenen kurzen Anweisungen umsetzbar sind wie z. B. eine Richtlinie zur Systemhärtung oder ein Konzept zur Verschlüsselung zu erstellen.

Für Kategorie B verweist der israelische Ansatz auf eine „Control Bank“ und Online-Tools, die nur auf Hebräisch verfügbar sind. Auf Englisch ist jedoch eine Fassung als Excel-Tabelle verfügbar [71] (s. auch Anhang 0).

Inhaltlich ist dies eine eigenständige Sammlung von 120 Maßnahmen mit zugehörigen Konkretisierungen. Sie ist weder in Anlehnung an das NIST CSF noch an ISO/IEC 27001 gegliedert und verfolgt offenbar das Ziel, bei ähnlich kompaktem Umfang wie ISO/IEC 27002 konkretere Handlungsanweisungen zu geben und nationale Besonderheiten in der Bedrohungslage zu berücksichtigen. Veranschaulichende Beispiele zu dieser Einschätzung sind im Anhang 0.

4.15.3 Zusammenfassende Bewertung

Der israelische Ansatz ist ein seiner aktuellen Form „Cyber Defense Doctrine 2.0“ von 2021 ein eigenständiger, unabhängig von anderen Standards, während die

Vorgängerversion „Cyber Defense Methodology for an Organization 1.0“ von 2017 sich noch eng am NIST CSF 1.1 orientierte.

Die Zweiteilung für zwei Organisationsgrößen entspricht einem üblichen Muster, für kleine Organisationen direkt eine Auswahl von Maßnahmen umzusetzen und für größere Organisationen risikobasiert und unter Anwendung eines vordefinierten Katalogs zu entscheiden. Die genannte Grenze zwischen beiden Ansätzen erscheint dabei willkürlich und in der Beurteilung, ob sie überschritten ist oder nicht, mit großen Unsicherheiten und Ermessensspielraum behaftet.

In der Vorgehensweise finden sich keine gegenüber den anderen betrachteten Ansätzen neuartigen und positiv hervorzuhebenden Aspekte. Zu erwähnen wäre die Variante der Risikobewertung, die jedoch nicht zur Aufgabenstellung gehört.

Die für Unternehmen der Kategorie A empfohlenen Maßnahmen muten – zumindest in dem auf Englisch veröffentlichten Material – aus o. g. Gründen nicht praktikabel an und sind daher nicht näher betrachtet.

Die für Unternehmen der Kategorie B empfohlenen Maßnahmen sind eigenständig formuliert und unabhängig von etablierten Standards. Sie enthalten ähnliche Breite an Maßnahmen wie ISO/IEC 27001, aufgeteilt in einen ebenfalls vergleichbaren Umfang von 120 generischen Controls – aber mit wesentlich konkreteren Umsetzungshinweisen dazu. Diese auszuwerten, würde den Umfang dieser Arbeit weit übersteigen, die Sammlung könnte jedoch bei der Erstellung von Umsetzungshinweisen zu anderen Standards möglicherweise wertvollen Input liefern.

4.16 Australien: Information Security Manual und Strategies to Mitigate Cyber Security Incidents

4.16.1 Überblick

Das australische **Information Security Manual (ISM)** [72] hat zum Ziel, „to outline a cyber security framework“, mit dem Unternehmen ihre Systeme und Daten vor Bedrohungen aus dem Cyberraum schützen können, unter

Verwendung eines vorhandenen Risikomanagements. Damit ist es ganz im Einklang mit diversen anderen Ansätzen und insbesondere dem NIST CSF und vorrangig an große Organisationen gerichtet.

Es ist ein PDF-Dokument von 177 Seiten und insgesamt über 900 Controls, damit umfangreicher als NIST CSF und ISO/IEC 27001 und 27002, aber deutlich kleiner als der deutsche IT-Grundschutz. Inhaltlich sind die Controls eigenständig formuliert, ohne Entsprechung in einem der gängigen Standards.

Zum Risikomanagement gibt das ISM keine konkreten Hinweise und verweist lediglich auf eine entsprechende Publikation SP 800-37 des NIST.

Daneben steht mit den **Strategies to Mitigate Cyber Security Incidents** ein grundlegend anderer Ansatz als alle bisher beschriebenen: Er greift vier konkrete und besonders relevante Bedrohungen von Cyberangriffen auf und beschreibt zugehörige Strategien, wie diesen begegnet werden kann. Die Strategien sind zum einen verlinkt in weiterführende und sehr konkrete Umsetzungshinweise sowie teilweise in die Controls des Information Security Manual.

4.16.2 Information Security Manual

Format

Das australische Information Security Manual (ISM) ist über eine eigene Webseite veröffentlicht [73]. Alle Inhalte sind als Webseite und PDF-Dokument verfügbar:

- eine gesammelte Publikation des vollständigen ISM als PDF-Dokument auf der zuvor genannten Webseite
- alle einzelnen Kapitel des ISM sind als „Guidelines“ auf eigenen Unterseiten und dort auch als herunterladbares PDF-Dokument verfügbar.

Die insgesamt 906 Controls sind zusätzlich als separates Excel-Sheet “System Security Plan” verfügbar [74].

Sicherheitsmaßnahmen

Am Anfang stehen 24 **Principles**, die strategische Orientierung bieten, gegliedert in vier vom NIST CSF bekannte Kategorien: Govern, protect, detect, respond. Sie bieten eine gute strategische Orientierung und sind sorgfältig formulierte, sinnvolle strategische Leitlinien, können Grundlage für die Definition eigener Maßnahmen sein (s. Anhang 0). Sie stehen aber unabhängig von den zahlreichen nachfolgenden Controls.

Die restliche Gliederung geschieht über sog. **Guidelines**, d. h. 22 einzelne Kapitel, bezeichnet als „Guideline for …“. Sie bringen einen neuen Aspekt mit erheblichem praktischen Nutzen: Guidelines lassen sich direkt als Vorlage für entsprechende Vorgabedokumente in Form von Richtlinien verwenden. Die Themen der Kapitel decken die typischen, von den NIST- und ISO-Publikationen sowie anderen behandelten Standards bekannten Bereiche ab, z. B. Sicherheitsorganisation, Sicherheitsvorfälle, Beschaffung und Outsourcing, physische Sicherheit etc. Eine vollständige Liste der Kapitel ist im Anhang 0.

Die Erstellung eigener Richtlinien ist trotzdem noch erforderlich und an einzelnen Stellen sogar gefordert, der Aufwand dafür aber deutlich reduziert.

Innerhalb der Kapitel bzw. Guidelines finden sich die erwähnten insgesamt über 900 Controls wieder, gegliedert in „Sections“ und „Topics“, ein Topic kann dabei eine oder mehrere Controls haben:

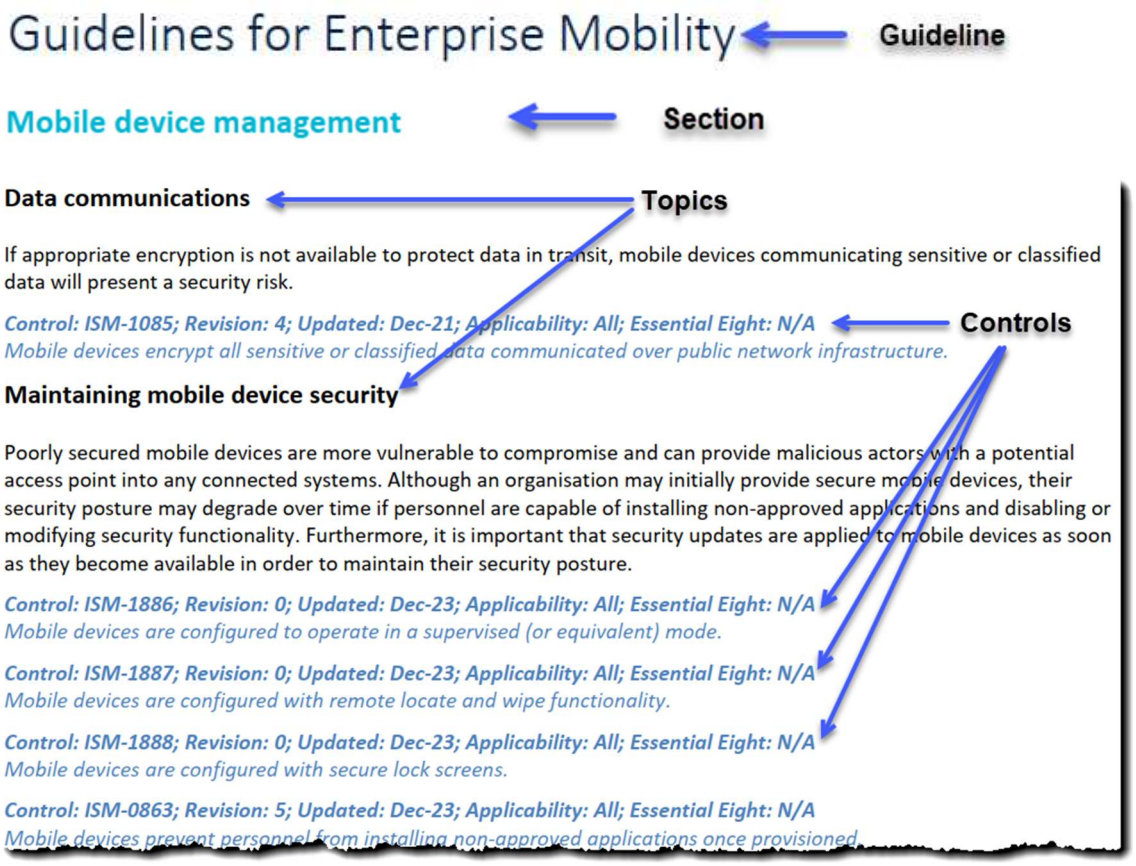


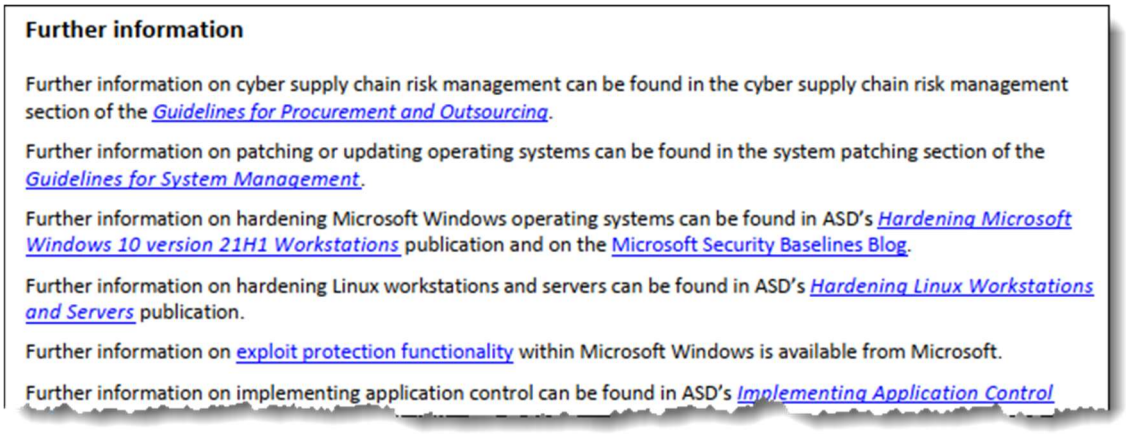
Abbildung 29: Beispiel eines Topics aus dem australischen ISM, Kapitel "Guidelines for Enterprise Mobility"
Quelle: [72, S. 53]

- Die „Topics“ gliedern die Controls in überschaubar kleine Themen und bieten erläuternden Text dazu an.
- Die Controls selber sind ergebnisorientiert, überprüfbar und knapp formuliert.
- Zu einem Topic können eine oder mehrere Controls existieren – oder mitunter gar keine; die Struktur der Guidelines lässt auf diese Weise Kapitel mit rein erläuterndem Text zu.
- Die Controls haben eindeutige Referenzen und Versionierungen mit Zeitstempel. Dadurch sind laufende Aktualisierungen auf Ebene einzelner Controls möglich. Gleichzeitig kann jeder Anwender des ISM nachvollziehen, wo sich Änderungen gegenüber einem in der jeweiligen Organisation verwendeten Stand ergeben haben.

Die numerischen IDs haben dabei keine Logik oder Aussagekraft in ihrer Nummerierung, sie werden fortlaufend nach Erscheinen vergeben und dienen nur der eindeutigen Identifizierung.

- Jede Control hat Hinweise zur Anwendbarkeit („Applicability“), die bei Bedarf anzeigt, ob Controls nur für bestimmte Klassifizierungen von staatlicher Vertraulichkeitsstufen relevant sind und ob sie den weiter unten erklärten „Essential Eight“ angehören.

Am Ende vieler Abschnitte („Sections“) führen Links zu weiteren Informationen, entweder zu weiteren Veröffentlichungen der australischen Cybersicherheits-Behörde oder externen Quellen, die direkt sehr konkrete und produktbezogene Umsetzungshilfen darstellen; hier ein Beispiel aus dem Kapitel zur Systemhärtung:



Further information

Further information on cyber supply chain risk management can be found in the cyber supply chain risk management section of the *Guidelines for Procurement and Outsourcing*.

Further information on patching or updating operating systems can be found in the system patching section of the *Guidelines for System Management*.

Further information on hardening Microsoft Windows operating systems can be found in ASD's *Hardening Microsoft Windows 10 version 21H1 Workstations* publication and on the Microsoft Security Baselines Blog.

Further information on hardening Linux workstations and servers can be found in ASD's *Hardening Linux Workstations and Servers* publication.

Further information on exploit protection functionality within Microsoft Windows is available from Microsoft.

Further information on implementing application control can be found in ASD's *Implementing Application Control*

Abbildung 30: Beispiel weiterführender Informationen aus dem australischen ISM, zum Thema Systemhärtung
Quelle: [72, S. 81]

Damit schafft das ISM eine Verbindung zu sehr operativen Anleitungen, wo es sinnvoll ist.

Vorgehensweise

Das australische ISM enthält eine auf nur zwei Seiten beschriebene simple Vorgehensweise, basierend auf dem amerikanischen Modell für Risikomanagement NIST SP 800-37:

- **Define the system** – Dabei ist es gleich, was als „System“ zugrunde liegt, dies ist Entscheidung der jeweiligen Organisation. Entsprechend lassen sich kleine oder große Teilbereiche betrachten.

Diese Vorgehensweise und beliebige Festlegung des Geltungsbereichs entspricht dem NIST CSF und auch z. B. dem Schweizer Ansatz.

- **Select controls** – Im Ergebnis ist ein „system security plan“ zu dokumentieren, der aus allen gelisteten Controls die relevanten auswählt und risikobasiert ggf. ergänzt. Dazu sind alle Controls des ISM in Tabellenform verfügbar und jede Guideline enthält Hinweise zu möglichen Risiken.
- **Assess controls** – Bewertung des aktuellen Stands von als relevant bewerteten Sicherheitsmaßnahmen.
- **Authorise the system** – Freigabe des Systems und Akzeptanz der Restrisiken.
- **Monitor the system** – laufende Beobachtung und ggf. Anpassung.

4.16.3 Strategies to Mitigate Cyber Security Incidents

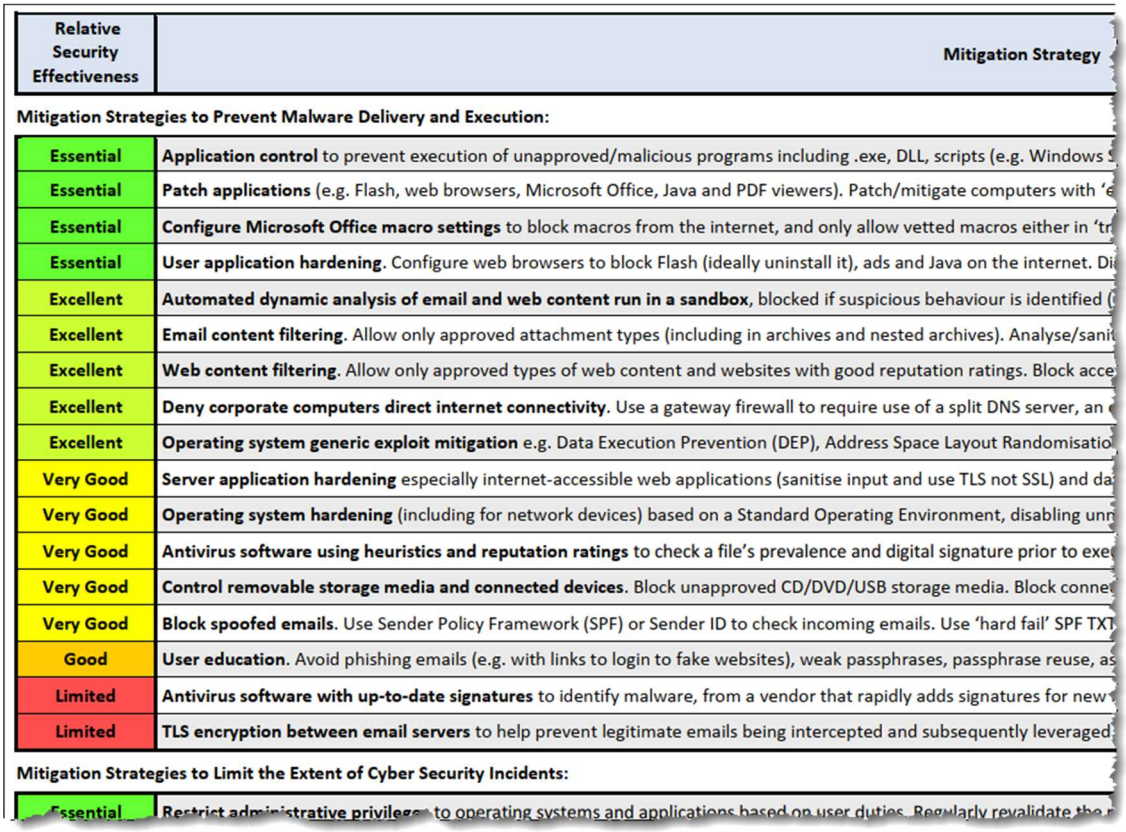
Die “Strategies to Mitigate Cyber Security Incidents” [75] basieren auf vier als besonders relevant erachteten Gefährdungen:

- Cyberattacken von Angreifern, die Daten stehlen möchten
- Ransomware-Attacken
- Angriffe von Innentätern, die Daten stehlen möchten
- Angriffe von Innentätern, die Daten zerstören oder Computer und Netzwerke sabotieren möchten.

Zur Verhinderung und Eindämmung dieser Risiken stellt der Ansatz fünf Arten von Strategien vor, die folgende Schwerpunkte haben:

- Prevent: Verhinderung von Schadsoftware-Installation und -Ausführung
- Contain: Begrenzung der Auswirkungen von Cybersicherheits-Vorfällen
- Detect: Entdecken von Cybersicherheits-Vorfällen und Reaktion darauf
- Recover: Wiederherstellung von Systemen
- Verhinderung von Innentätern.

Zur Veranschaulichung hier ein Ausschnitt der Strategien zur Verhinderung von Schadsoftware-Installation und Ausführung:



Relative Security Effectiveness	Mitigation Strategy
Mitigation Strategies to Prevent Malware Delivery and Execution:	
Essential	**Application control** to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows
Essential	**Patch applications** (e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers). Patch/mitigate computers with 'e
Essential	**Configure Microsoft Office macro settings** to block macros from the internet, and only allow vetted macros either in 'tr
Essential	**User application hardening**. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the internet. Di
Excellent	**Automated dynamic analysis of email and web content run in a sandbox**, blocked if suspicious behaviour is identified (
Excellent	**Email content filtering**. Allow only approved attachment types (including in archives and nested archives). Analyse/sani
Excellent	**Web content filtering**. Allow only approved types of web content and websites with good reputation ratings. Block acce
Excellent	**Deny corporate computers direct internet connectivity**. Use a gateway firewall to require use of a split DNS server, an
Excellent	**Operating system generic exploit mitigation** e.g. Data Execution Prevention (DEP), Address Space Layout Randomisatio
Very Good	**Server application hardening** especially internet-accessible web applications (sanitise input and use TLS not SSL) and da
Very Good	**Operating system hardening** (including for network devices) based on a Standard Operating Environment, disabling unn
Very Good	**Antivirus software using heuristics and reputation ratings** to check a file's prevalence and digital signature prior to exe
Very Good	**Control removable storage media and connected devices**. Block unapproved CD/DVD/USB storage media. Block connec
Very Good	**Block spoofed emails**. Use Sender Policy Framework (SPF) or Sender ID to check incoming emails. Use 'hard fail' SPF TXT
Good	**User education**. Avoid phishing emails (e.g. with links to login to fake websites), weak passphrases, passphrase reuse, as
Limited	**Antivirus software with up-to-date signatures** to identify malware, from a vendor that rapidly adds signatures for new
Limited	**TLS encryption between email servers** to help prevent legitimate emails being intercepted and subsequently leveraged
Mitigation Strategies to Limit the Extent of Cyber Security Incidents:	
Essential	**Restrict administrative privileges** to operating systems and applications based on user duties. Regularly revalidate the

Abbildung 31: Ausschnitt der Strategies to Mitigate Cyber Security Incidents
Quelle: [75]

Zu erkennen ist, dass die Strategien allgemeine Handlungsanweisungen wie z. B. die Kontrolle von Programmausführungen, Patch-Management usw. enthalten. Zusätzlich sind ihnen Einstufungen der Wirksamkeit zugeordnet, mit „Essential" als dem höchsten Wert, darunter Excellent, Very Good, Good und Limited.

Die Strategien ergänzen sich, es können aus jedem Bereich beliebig viele umgesetzt werden.

Für jede der vier Gefährdungen gibt der Ansatz dann Empfehlungen, welche Arten von Strategien dafür vorrangig implementiert werden sollten, z. B. für die erste Gefährdung:

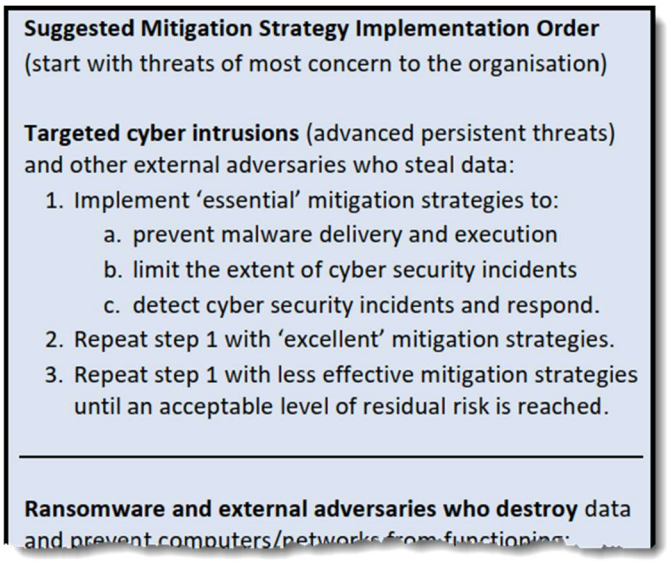


Abbildung 32: Empfohlene Strategien gegen gezielte Cyberangriffe mit dem Ziel, Daten zu stehlen
Quelle: [75]

Zu erkennen ist, dass der Ansatz für jede Bedrohung eine Auswahl von Strategien empfiehlt, hier zunächst die als „Essential" bewerteten aus drei der Bereiche, anschließend die als weniger wirksam bewerteten. Die Empfehlungen für andere Bedrohungen variieren leicht.

Für die konkrete Umsetzung aller Strategien gibt es zusätzliche konkrete Hinweise, sog. „Mitigation Details" [76].

4.16.4 Essential Eight

Die „Essential Eight" [77] sind ein Ergebnis des zuvor beschriebenen Ansatzes, die acht insgesamt als besonders wirksam bewerteten Strategien. Die Einschätzung basiert auf den Erfahrungen der Australischen Cybersicherheits-Behörde, Penetration Testung und beobachteten Sicherheitsvorfällen. Die australische Cybersicherheits-Behörde misst diesen Strategien große Bedeutung bei, definiert sie als „new cyber security baseline for all organisations".

Für sie gibt es eine weitere konkrete Umsetzungshilfe: Die Controls des Information Security Manual haben Referenzen zu den „Essential Eight" und zeigen konkret an, welche Maßnahmen für ihre Umsetzung erforderlich sind.

Das führt zu einer handhabbaren Anzahl von Controls:

- 46 für ein „Maturity Level“ (=Reifegrad) von 1
- 87 für ein Maturity Level 2
- 123 für Maturity Level 3.

Zur Überprüfung des Umsetzungsgrades der Essential Eight existiert eine weitere Publikation [78] mit konkreten Hinweisen. Diese sind auffallend detailliert, bis hin zur Angabe von PowerShell-Skripts, die Systeminformationen abfragen.

4.16.5 Zusammenhänge

Die nachfolgende Grafik veranschaulicht abschließend, wie die beschriebenen australischen Ansätze zusammenhängen:

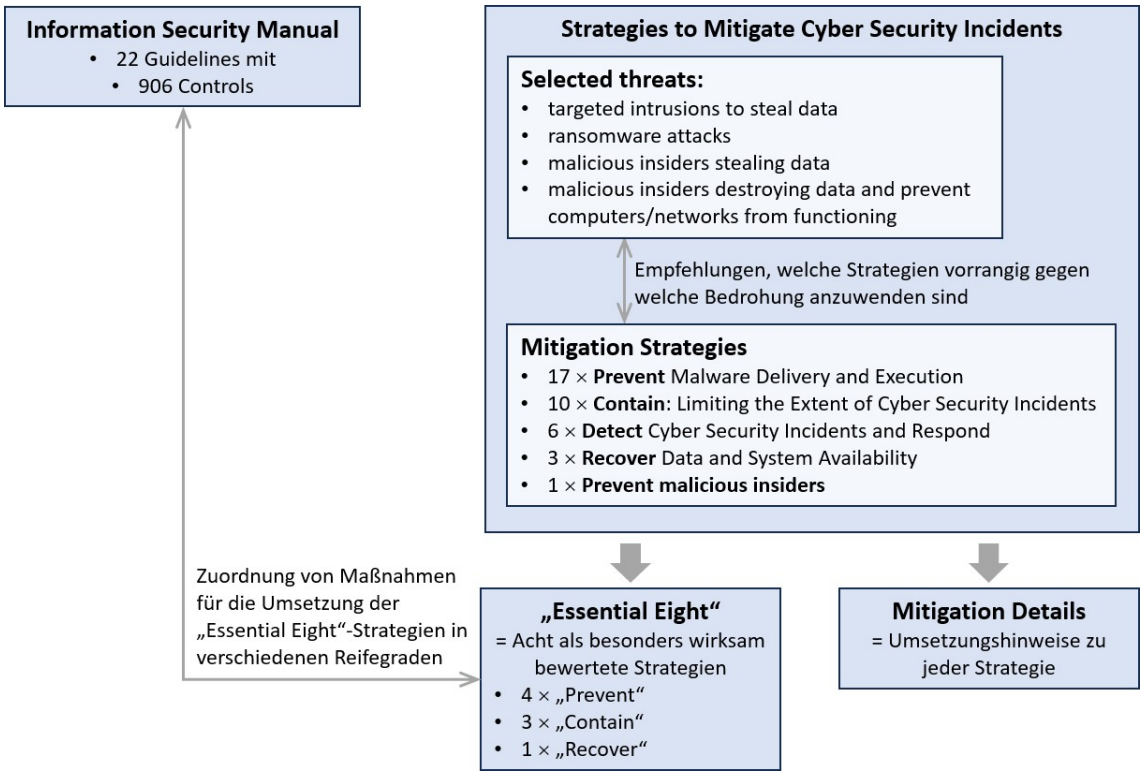


Abbildung 33: Zusammenhang der australischen Ansätze Information Security Manual, Strategies to Mitigate Cyber Security Incidents und Essential Eight
Quelle: Eigene Darstellung

- Hauptelemente sind die Publikationen
  - **Information Security Manual** mit der beschrieben umfangreichen Sammlung von Sicherheitsmaßnahmen, gegliedert in „Guidelines“
  - **Strategies to Mitigate Cyber Security Incidents** definieren auf hohem Abstraktionsniveau mögliche Vorgehensweisen gegen die wichtigsten

Cyberattacken mit den Zielrichtungen Prevent, Contain, Detect und Recover sowie einer Strategie gegen Innentäter.

- Zu den Strategien gibt es ergänzende Umsetzungshinweise in Form der „**Mitigation Details**“ und recht konkreten Handlungsanweisungen.
- Eine Teilmenge von als besonders wirksam erachteten Strategien sind als die „**Essential Eight**“ besonders hervorgehoben. Für sie existieren zusätzlich Referenzen in den Controls des Information Security Manual, die klar anzeigen, welche Maßnahmen zur Umsetzung dieser Strategien erforderlich sind.

Das Australian Cyber Directorate empfiehlt, beide Ansätze ISM und Essential unabhängig voneinander zu betrachten. Das ISM basiert vorrangig auf dem generellen Schutz der Vertraulichkeit verarbeiteter Daten; die Essential Eight auf Maßnahmen gegen verschiedene Stufen von Cyberangriffen. Dies sind unterschiedliche Blickwinkel und eine Organisation sollte bewusst aus beiden auswählen.

4.16.6 Zusammenfassende Bewertung

Der australische Ansatz sticht unter allen bisher betrachteten als ein eigenständiger mit einer Reihe von besonderen Merkmalen hervor:

- Seine **Balance aus Umfang und Abstraktionsgrad** bzw. Konkretheit seiner Maßnahmen erscheint ausgewogener als bei den etablierten Standards.
  - Der Textumfang positioniert ihn in einer Lücke oberhalb von ISO/IEC 27002, aber deutlich unterhalb des deutschen IT-Grundschutzes. Trotzdem sind die in ihm aufgelisteten Maßnahmen zusammen mit weiterführenden Links deutlich konkreter und leichter in Handlungen umsetzbar als im IT-Grundschutz.
  - Auf gleiche Weise liegt er zwischen dem NIST Cybersecurity Framework und NIST SP 800-53, mit noch deutlicheren Abständen.
- Die **Gliederung in Guidelines**, die als direkte Vorlage für Richtlinien können, eliminieren einen erheblichen Arbeitsaufwand in der Umsetzung für die Strukturierung der Vorgabedokumente und ihre Erstellung. Die Anordnung der Controls in einer für Richtlinien verwendbaren Form ist logisch und

naheliegend; weder NIST CSF, noch ISO/IEC 27001 und der deutsche IT-Grundschutz bieten diese Orientierung.

- Die innere **Struktur der Guidelines** bietet weitere Vorteile, die andere Ansätze nicht aufweisen:
  - Die knapp und als nachprüfbare Anforderungen formulierten Controls stehen direkt neben erläuternden Texten. Das verbindet leichte Nachvollziehbarkeit für eine Gap-Analyse und Umsetzungsplanung mit Hilfen zum Verständnis der Anforderungen.
  - Die Controls haben jede für sich eine Versionierung und Aktualisierungsdatum. Es ist so eine nachvollziehbare, kontinuierliche Aktualisierung einzelner Maßnahmen möglich; ein wesentlich flexiblerer Ansatz verglichen mit den bisher jährlichen Updates des Grundschutz-Kompendiums und noch längeren Zyklen im NIST CSF und ISO/IEC 27001 bzw. 27002.
  - Auf diese Weise bekommen Vorgabedokumente in Form von Richtlinien ebenfalls nachprüfbare, systematisch auswertbare Anforderungen – ein deutlicher Vorteil gegenüber der üblichen in der Praxis beobachteten Formulierung in Form reiner Fließtext-Dokumenten.
- Die ergänzenden **Strategien** sind eine wertvolle Ergänzung, ein anderer und neuer Blickwinkel auf Cyber-Sicherheitsmaßnahmen:
  - Sie sind direkt verknüpft mit äußerst relevanten Bedrohungen in Form gängiger Cyber-Attacken und geben Orientierung bezüglich der Wirksamkeit gegen diese Bedrohungen – wertvolle Zuarbeit für die von allen Ansätzen geforderte risikobasierte Betrachtungsweise. Welche Maßnahmen konkret gegen welche Bedrohungen bei Cyber-Attacken helfen, obliegt bei allen anderen Ansätzen dem Urteil der jeweiligen Organisation, es ist aber ein Schlüssel für wirksame Abwehrmaßnahmen und eine Basis-Information, die man sich von einem veröffentlichten standardisierten Ansatz wünscht.
  - Die Unterteilung der häufig zitierten Schutzfunktion „Protect“ aus dem NIST CSF in „prevent“ und „contain“ ist eine sinnvolle und einleuchtende.
  - Die Brücke von den Abwehrstrategien zu konkreten Umsetzungshinweisen – in Form von zusätzlichen, trotz konkreter Hinweise übersichtlich kurzer

Dokumente – sowie mit Verknüpfung der „Essential Eight“-Strategien zu Controls des ISM ist vorbildlich.

Der zweigleisige Ansatz über das ISM und die Strategien ist sehr sinnvoll, beide ergänzen sich gut.

Im deutschen Grundschutz stecken mit seiner integrierten Risikoanalyse zwar ähnliche Gedanken, aber sie behandeln nur die generischen 47 G 0-Gefährdungen, die nicht vergleichbar mit den konkret ausgewählten Formen von Cyber-Attacken im australischen Ansatz sind. Zudem ist die Brücke von Gefährdungen zu Maßnahmen im IT-Grundschutz nur äußerst mühsam über sog. Kreuzreferenztabellen möglich. Diese zeigen zu jedem Baustein an, welche Anforderungen gegen welche Gefährdungen geeignet sind. Sie sind jedoch nur im Text der vielen Kompendium-Bausteine und als Excel-Tabelle mit einem Arbeitsblatt je Baustein – insgesamt also über 100 – verfügbar.

Eine einfacher handzuhabende Form der Kreuzreferenztabellen hätte das Potential, beliebige Gefährdungen zu ergänzen und mit Maßnahmen zu verknüpfen und so eine vergleichbar mächtige Funktion zu liefern.

4.17 Saudi-Arabien: Essential Cybersecurity Controls

4.17.1 Überblick

Die Essential Cybersecurity Controls (ECC) definieren nationale Mindestanforderungen für alle staatlichen Organisationen in deren Geltungsbereich. Sie sind laut königlichem Dekret für alle staatlichen Organisationen in Saudi-Arabien allesamt verpflichtend.

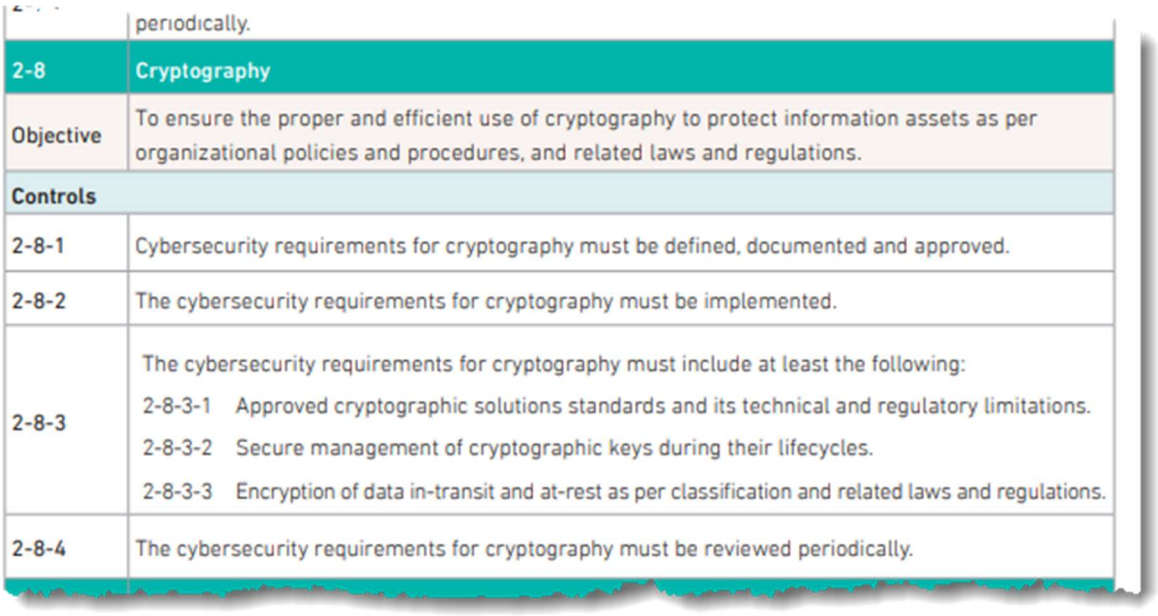
Sie sind nach eigener Aussage basierend auf einer gründlichen Betrachtung internationaler Standards, aber eigenständig formuliert.

4.17.2 Inhaltliche Beschreibung

Das Hauptdokument der Essential Cybersecurity Controls [79] ist mit 40 Seiten im Umfang vergleichbar der ISO/IEC 27001 und listet eine ähnliche Anzahl von

114 Controls, gegliedert in 5 Domains und 29 Subdomains. Eine Übersicht ist im Anhang 0, insgesamt decken sie sich im Umfang mit ISO/IEC 27001, eingegrenzt auf Cybersicherheit.

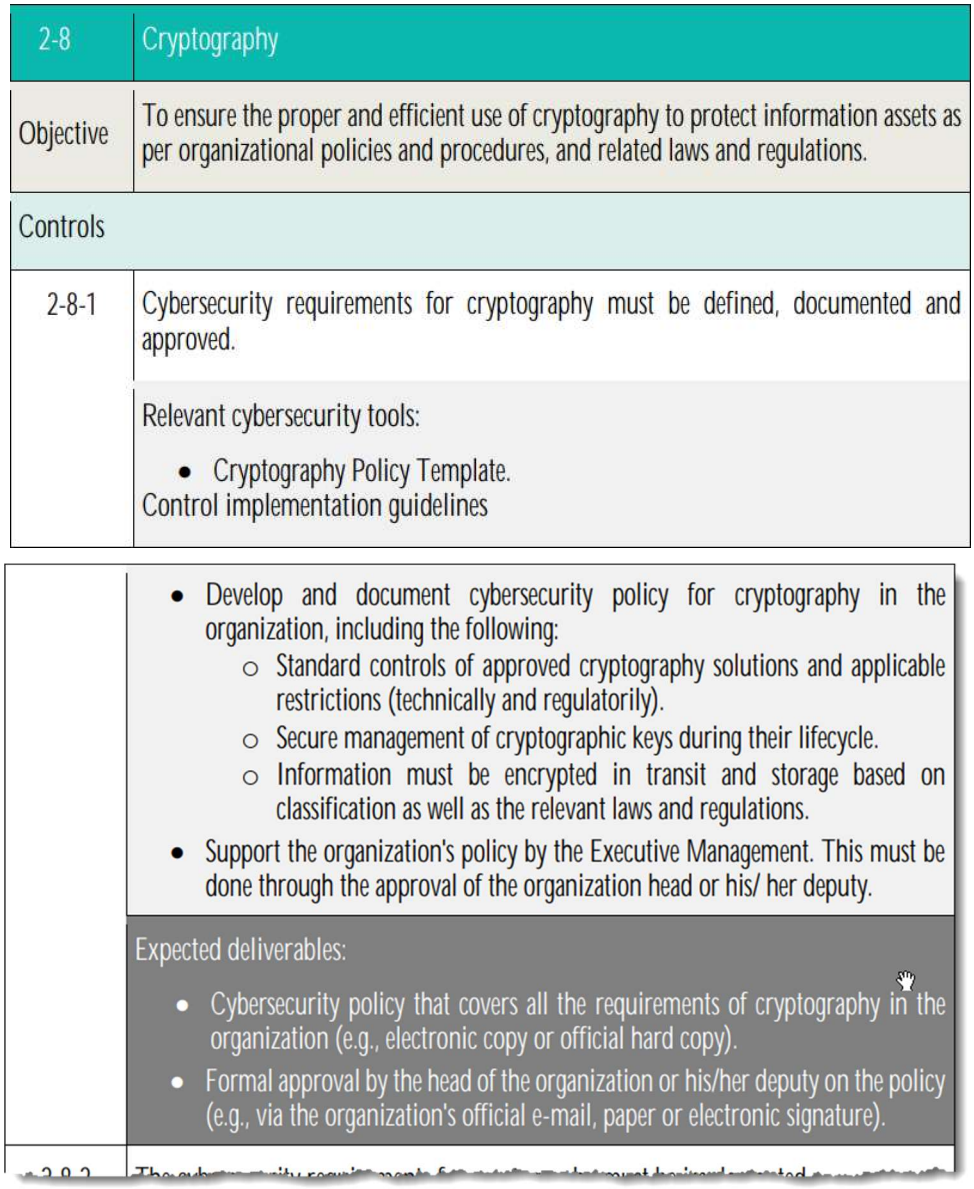
Nachfolgend ein Beispiel zur Veranschaulichung des Abstraktionsgrades:



	periodically.
2-8	**Cryptography**
Objective	To ensure the proper and efficient use of cryptography to protect information assets as per organizational policies and procedures, and related laws and regulations.
Controls	
2-8-1	Cybersecurity requirements for cryptography must be defined, documented and approved.
2-8-2	The cybersecurity requirements for cryptography must be implemented.
2-8-3	The cybersecurity requirements for cryptography must include at least the following: 2-8-3-1 Approved cryptographic solutions standards and its technical and regulatory limitations. 2-8-3-2 Secure management of cryptographic keys during their lifecycles. 2-8-3-3 Encryption of data in-transit and at-rest as per classification and related laws and regulations.
2-8-4	The cybersecurity requirements for cryptography must be reviewed periodically.

Abbildung 34: Beispiel von Controls mit drei Sub-Controls aus den saudi-arabischen ECC
Quelle: [79, S. 22]

Zu allen Controls existieren **Umsetzungshinweise** in einem separaten Dokument „Guide to Essential Cybersecurity Controls (ECC) Implementation“ [80]. Es gibt zu jeder Control Umsetzungshinweise und definiert dafür zu erstellende Ergebnisse; nachfolgend zu dem Punkt 2-8-1 des obigen Ausschnitts gehörende Erläuterungen:



2-8	Cryptography
Objective	To ensure the proper and efficient use of cryptography to protect information assets as per organizational policies and procedures, and related laws and regulations.
Controls	
2-8-1	Cybersecurity requirements for cryptography must be defined, documented and approved.
	Relevant cybersecurity tools: • Cryptography Policy Template. Control implementation guidelines
	• Develop and document cybersecurity policy for cryptography in the organization, including the following: ○ Standard controls of approved cryptography solutions and applicable restrictions (technically and regulatorily). ○ Secure management of cryptographic keys during their lifecycle. ○ Information must be encrypted in transit and storage based on classification as well as the relevant laws and regulations. • Support the organization's policy by the Executive Management. This must be done through the approval of the organization head or his/ her deputy.
	Expected deliverables: • Cybersecurity policy that covers all the requirements of cryptography in the organization (e.g., electronic copy or official hard copy). • Formal approval by the head of the organization or his/her deputy on the policy (e.g., via the organization's official e-mail, paper or electronic signature).

Abbildung 35: Beispiel von Umsetzungshinweisen zu Controls der ECC
Quelle: [80, S. 101]

Der saudi-arabische Ansatz geht anschließend einen Schritt weiter, indem er **Templates für alle erwähnten Vorgabedokumente** zur Verfügung stellt, die alle Anforderungen abdecken und nur noch mit organisationsspezifischen Details wie Namen und Funktionsbezeichnungen zu bearbeiten sind [81]. Dieses „Cybersecurity Toolkit“ ist eine Sammlung von über 80 Dokumenten, vor allem sog. „Policies“ die „cybersecurity requirements“ für ein bestimmtes Thema definieren und „Standards“, die „detailed cybersecurity requirements“ für ein Thema vorgeben. Eine durchgängige Nummerierung referenziert die zugehörigen Subdomains:

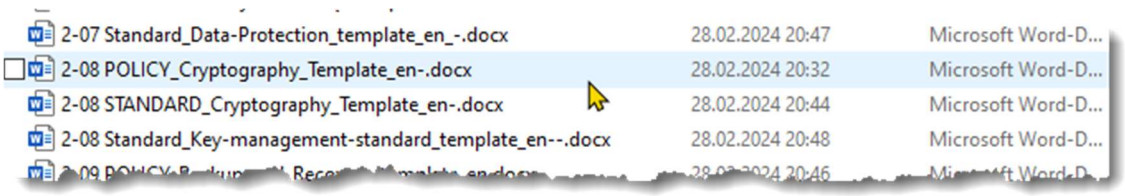
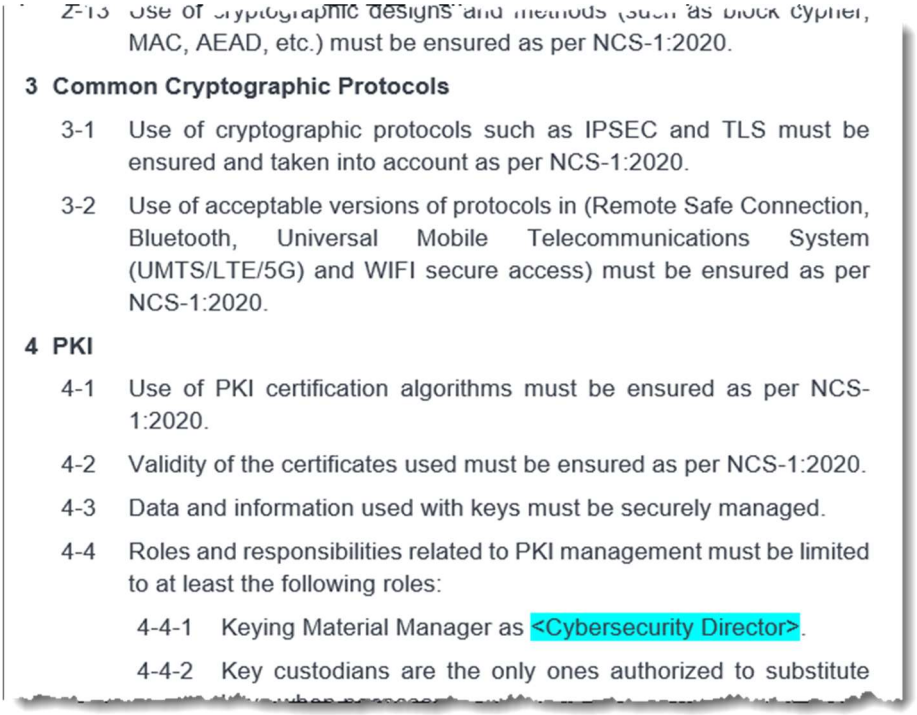


Abbildung 36: Beispielhafte Templates des saudi-arabischen Cybersecurity-Toolkits
Quelle: [81].

Die Vorgabedokumente enthalten wiederum durchgängig nummerierte Regelungen, die oft recht weit ins Detail gehen, hier ein Ausschnitt aus der zum obigen Beispiel gehörenden Policy zum Thema Verschlüsselung:



Z-13 Use of cryptographic designs and methods (such as block cypher, MAC, AEAD, etc.) must be ensured as per NCS-1:2020.

3 Common Cryptographic Protocols

3-1 Use of cryptographic protocols such as IPSEC and TLS must be ensured and taken into account as per NCS-1:2020.

3-2 Use of acceptable versions of protocols in (Remote Safe Connection, Bluetooth, Universal Mobile Telecommunications System (UMTS/LTE/5G) and WIFI secure access) must be ensured as per NCS-1:2020.

4 PKI

4-1 Use of PKI certification algorithms must be ensured as per NCS-1:2020.

4-2 Validity of the certificates used must be ensured as per NCS-1:2020.

4-3 Data and information used with keys must be securely managed.

4-4 Roles and responsibilities related to PKI management must be limited to at least the following roles:

4-4-1 Keying Material Manager as <Cybersecurity Director>.

4-4-2 Key custodians are the only ones authorized to substitute

Abbildung 37: Ausschnitt aus Policy_Cryptography_Template_en.docx
Quelle: [81]

Ein Risikomanagement mit einem Verweis auf die Standards von ISO/IEC und NIST ist auch Teil der vorgeschriebenen Maßnahmen, hat aber nur die Aufgabe zusätzliche Maßnahmen zu finden und Restrisiken zu dokumentieren.

4.17.3 Zusammenfassende Bewertung

Die zwei Hauptdokumente, Essential Cybersecurity Controls (ECC) und Guide to ECC Implementation liefern einen umfassenden Katalog an Sicherheitsmaßnahmen, einmal auf 40 Seiten überschaubar und mit hohem Abstraktionsgrad und ergänzend mit diversen Erläuterungen wie in der ISO/IEC 27002.

Eine entscheidende und bei keinem anderen Ansatz vorhandene Erweiterung ist das Cybersecurity Toolkit, das konsistent mit allen Umsetzungshinweisen des „Guide to Implementation“ einen umfangreichen Satz von vorformulierten Vorgabedokumenten bereitstellt.

Damit gibt der saudi-arabische Ansatz als einziger einen kompletten und konsistenten Weg von generisch formulierten Maßnahmen wie in der ISO/IEC 27001 in Richtung der konkreten Umsetzung. Der Ansatz ist sehr konsequent und nachvollziehbar umgesetzt, mit klaren Referenzen über alle Dokumente hinweg.

Die Aufteilung aller Vorgabedokumente in nummerierte und übersichtlich klein gegliederte Regelungen ist ebenfalls positiv zu erwähnen, für eine systematische Nachverfolgung und Umsetzungsplanung.

Die Struktur der Vorgabedokumente und viele Teile ihrer Inhalte können durchaus als Input und Orientierung für die Umsetzung der anderen Standards sinnvoll verwendet werden.

Sie zielen darauf ab, einen einheitlichen hohen Standard an Cybersicherheit zu erreichen – ohne Flexibilität und Wahlmöglichkeiten und orientiert an großen Organisationen, wie sich z. B. an der vorgeschlagenen Organisationsstruktur mit einem eigenen „Cybersecurity Department“ erkennen lässt.

4.18 Vereinigtes Königreich: Cyber Essentials

4.18.1 Überblick

Die „Cyber Essentials“ [82] sind eine kurze Sammlung konkreter Maßnahmen für eine Mindestabsicherung gegen die häufigsten Cyberattacken, für Organisationen beliebiger Art und Größe.

4.18.2 Inhaltliche Beschreibung

Die Cyber Essentials sind auf überschaubaren 16 Seiten beschrieben und verlangen zunächst eine simple Abgrenzung des Anwendungsbereichs, vergleichbar mit einer Inventarisierung:

- Abgrenzung nach außen, d. h. Ermitteln aller Schnittstellen und Übergänge
- aller für die Tätigkeit der Organisation notwendigen digitalen Geräte innerhalb des Anwendungsbereichs.

Innerhalb des Anwendungsbereichs sind grundlegende technische Anforderungen zu erfüllen, gegliedert in fünf Bereiche:

- Firewalls
- Sichere Konfiguration von Servern, Endgeräten und Cloud-Services
- Sicherheitsupdates
- Zugangsberechtigungen
- Schutz vor Schadsoftware.

In jedem Bereich finden sich eine kleine Zahl von ca. fünf Maßnahmen mit anschaulichen Erklärungen; als Beispiel sind diejenigen für Sicherheitsupdates im Anhang 0 gezeigt.

Die Cyber Essentials konzentrieren sich auf die so definierten Maßnahmen, ohne begleitende Risikoanalyse, ohne vorgeschriebene Vorgabedokumente.

Drei weitere Merkmale heben diesen Ansatz von vergleichbaren anderen ab:

- Es ist eine Zertifizierung möglich.
- Eine Zertifizierung nach diesem (oder einem mindestens vergleichbaren) Standard ist seit 2014 eine Mindestanforderung bei der Vergabe von staatlichen Aufträgen [83].
- Er unterstützt Interessenten mit einem interaktiven Online-Tool, das durch eine Reihe von Fragen führt und gezielte weitere Hilfestellungen gibt.

Eine Zertifizierung ist sonst nur von dem wesentlich umfangreicheren ISMS nach ISO/IEC 27001 oder IT-Grundschutz bekannt, nicht für solche wenigen essentiellen Absicherungen. Die Art der Zertifizierung ist sinnvoll zweigeteilt, für

eine gute Balance aus Aufwand und Nutzen und mit einem niedrigschwelligen Einstieg:

- Im einfacheren Fall erfolgt eine Selbsteinschätzung anhand einer Reihe von Fragen, verifiziert durch automatisierte Schwachstellen-Scans von außen und auf einer Stichprobe von Endgeräten; Kosten dafür liegen im Bereich von einigen Hundert britischen Pfund.
- Alternativ gibt es als „Cyber Essentials Plus“ eine Prüfung gegen dieselben Anforderungen, aber mit mehr Prüftiefe („hands on technical verification“) durch einen externen Auditor.

Die Verankerung dieses Standards in Vergabebedingungen für öffentliche Aufträge ist ein sinnvoller Weg, die Verbreitung von Cybersicherheit zu fördern und erscheint gut gelöst, da sie einen dadurch entstehenden Druck zur Einhaltung mit einem sinnvollen konkreten Angebot und vertretbarem Aufwand verbindet.

Das begleitende Online-Tool „Cyber Essentials Readiness Toolkit” [84] ist eine Arbeitshilfe, die Schritt für Schritt alle Anforderungen erläutert, abfragt und nur bei Bedarf Links zu weiterführenden Informationen anbietet. Als Ergebnis liefert die Webseite ein PDF-Dokument, das alle festgestellten Lücken zusammenfasst und direkt als Maßnahmenplan dienen kann.

Hier ein Beispiel zur Veranschaulichung:

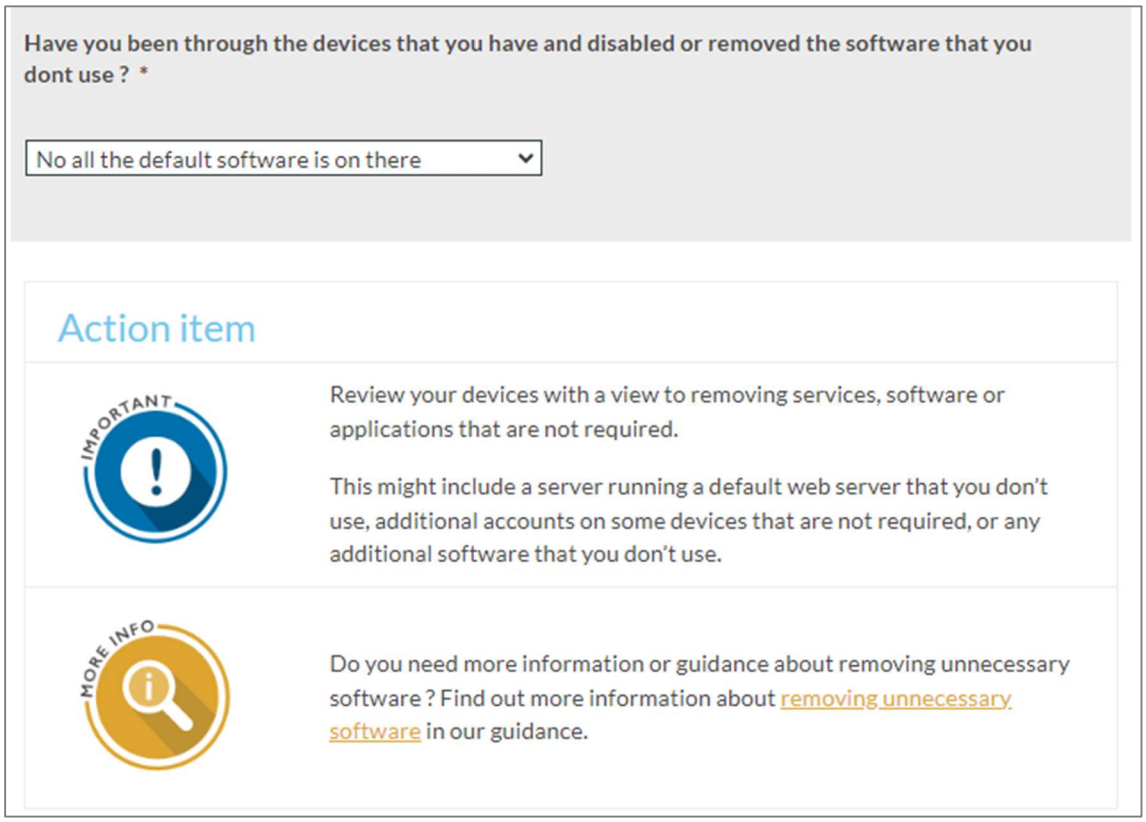


Abbildung 38: Beispielfrage aus „Cyber Essentials Readiness Toolkit“
Quelle: [84]

4.18.3 Zusammenfassende Bewertung

Die Festschreibung einer überschaubaren Zahl konkreter Maßnahmen ohne dazugehörige Risikobetrachtung ist für einen Einstieg in die Cybersicherheit zweifellos sinnvoll und bei den Cyber Essentials in guter Qualität und ansprechender Darstellung gelungen.

Darüber hinaus lassen die gezeigten Besonderheiten die Cyber Essentials als besonders gelungen erscheinen:

- Einfache Möglichkeit der Zertifizierung mit darin enthaltener automatisierter und technischer Überprüfung – nicht nur durch Befragung eines Auditors
- Förderung der Verbreitung durch Verankerung in Vergabebedingungen für öffentliche Aufträge
- Unterstützung mit einem einfachen Online-Tool, das eine einleuchtende, sehr konkrete praktische Arbeitshilfe darstellt.

4.19 Weitere Ansätze

4.19.1 Neuseeland: New Zealand Information Security Manual

Das „New Zealand Information Security Manual“ [85] ist eine umfangreiche Sammlung von Controls und Standard für Behörden und öffentliche Einrichtungen in Neuseeland. Es hat keine Referenzen zum NIST CSF oder ISO/IEC 27001 und eine anders strukturierte Gliederung, ist als eigenständiger Ansatz zu betrachten.

Sein Ziel ist „protection of all New Zealand Government information and systems” – damit ist es der einzige Vertreter der umfassenderen Informationssicherheit unter den nicht von ISO/IEC 27001 oder NIST CSF abgeleiteten Ansätzen.

Aufgrund seines Umfangs von 458 Seiten ist es nicht mehr mit einer genauen Betrachtung in diese Arbeit eingeflossen. Ein erstes Scannen der Inhalte ergab keine Anhaltspunkte für grundlegend neue Inhalte oder Ideen.

4.19.2 Singapur: Cyber Safe Programme

Das „Cyber Safe Programme“ aus Singapur [86] ist ein Ansatz, der Maßnahmen zur Cybersicherheit in verschiedenen Abstufungen anbietet:

- „Cyber Essentials“ für kleinere Organisationen oder solche mit wenigen digitalisierten Abläufen
- „Cyber Trust“ für größere Organisationen oder solche mit vielen digitalisierten Abläufen; weiter unterteilt in 5 Stufen („Tiers“), wobei die Anzahl der empfohlenen Maßnahmen mit jeder Stufe zunimmt.

Dieser Ansatz ist eine mit ISO/IEC 27001 kompatible Einstiegshilfe, indem er sinnvolle Umsetzungstiefen und damit -aufwände definiert. Ein Mapping zu ISO/IEC 27001 gibt an, in welcher Stufe welcher Anteil von Anforderungen enthalten ist. Dies reicht bis zu knapp 80 % der ISMS-Anforderungen aus Kap. 4 – 10 und 90 % aus Annex A. Für eine vollständige Abdeckung wäre dann eine Zertifizierung direkt basierend auf ISO/IEC 27001 erforderlich.

Die stufenweise Wahl eines Umsetzungsgrades ist ein sinnvoller Weg für Organisationen, die den Aufwand eines vollständigen ISMS scheuen. Inhaltlich bringt dieser Ansatz wegen seiner Nähe zu ISO/IEC 27001 keine neuen Aspekte und ist hier nicht im Detail betrachtet.

4.19.3 Neuseeland: Cyber Security Framework

Das neuseeländische Cyber Security Framework [87] ist eine nationale Adaption des NIST Cybersecurity Framework v1.1. Es strukturiert die fünf Funktionen anders, indem es mit einer zusätzlichen Funktion „Guide & Govern“ alle übergreifenden Verantwortlichkeiten der Leitungsebene zusammenfasst; dies nimmt die im NIST CSF 2.0 neu eingeführte Funktion „Govern“ vorweg. Gleichzeitig sind die separaten Funktionen „Respond“ und „Recover“ zusammengefasst.

Das Framework liegt aber erst in einer Beta-Version und mit einem 7-seitigen Übersichtsdokument vor, noch ohne weitere Details und kann daher nicht genauer betrachtet werden.

4.19.4 Schweiz: Branchenstandards

Die Schweizer Branchenstandards [88] definieren Minimalanforderungen für Informationssicherheit in ausgewählten Branchen der kritischen Infrastruktur. Sie basieren auf dem NIST CSF 1.1 und enthalten Cybersicherheits-Maßnahmen als Auswahl und Übersetzung von Anforderungen des NIST CSF.

In dieser Arbeit sind sie nicht mit einer genaueren Betrachtung berücksichtigt, da sie branchenspezifisch sind und damit nicht in die Abgrenzung der Aufgabenstellung fallen.

4.19.5 Irland: Public Sector Security Baseline Standards

Dieser irische Standard [89] ist ein Mindeststandard für Cybersicherheit bei allen öffentlichen Institutionen, basierend auf der Struktur des NIST CSF 1.1.

Er definiert auf 66 Seiten konkretere Anforderungen für jede der Funktionen als das NIST CSF in seinen categories und subcategories und hat auch eine andere Gliederung. Zudem sind die jeweiligen Anforderungen in verpflichtende und wahlweise umzusetzende unterschieden. Er ist daher eher ein eigenständiger Ansatz, gegliedert nach dem Vorbild des NIST CSF 1.1.

Eine genaue Betrachtung wurde nicht vorgenommen, da dies den Umfang dieser Arbeit übersteigen würde und ein erstes Sichten keine grundlegend neuen Inhalte oder Vorgehensweisen erkennen lässt.

4.19.6 Kanada: IT security risk management (ITSG-33)

Als „Information Technology Security Guidance“ (ITSG) hat die kanadische Regierung in 2012 einen immer noch gültigen Ansatz veröffentlicht: „IT Security Risk Management: A Lifecycle Approach (ITSG-33)“ [90]. Er beschreibt ein Vorgehen zum Risikomanagement und definiert als Annex 4A „Baseline Controls“, die wiederum eine Auswahl der amerikanischen NIST SP 800-53 sind.

Dieser Ansatz ist hier nicht detailliert betrachtet; eine oberflächliche Sichtung zeigte keine grundlegend neuen Inhalte.

4.19.7 Kanada: Baseline Cyber Security Controls

Die „Baseline Cyber Security Controls for Small and Medium Organizations“ [90] sind ein auf dem zuvor erwähnten ITSG-33 basierender, im Jahr 2020 erschienener Ansatz. Sie haben zum Ziel, diesen sehr aufwändigen nach der 80/20-Regel zu vereinfachen – ca. 80 % des Nutzens mit ca. 20 % des Aufwands zu erreichen und versteht sich als geeignet für Organisationen mit unter 500 Mitarbeitern.

Er ist mit 20 Seiten übersichtlich kurz und besteht aus einer reinen Sammlung von Sicherheitsmaßnahmen, in zwei Bereiche gegliedert:

- Organizational controls – eine vereinfachte Fassung organisationsweiter Maßnahmen z. B. zur Abgrenzung des Geltungsbereichs und der Kategorisierung von Assets

- Baseline Controls – die eigentlichen Sicherheitsmaßnahmen, gegliedert in 13 Bereiche.

Dieser Ansatz ist hier ebenfalls nicht detailliert betrachtet; er enthält gegenüber den bisher betrachteten Ansätzen keine grundlegend neuen Aspekte.

Die 13 Bereiche sind zusätzlich als „Top Measures to enhance cyber security for small and medium organizations“ zusammengefasst und separat veröffentlicht [91].

4.19.8 Dänemark: Effective Cyber Defence

Der dänische Ansatz „Effective Cyber Defence“ [92] ist ein mit 19 Seiten übersichtlich kurzer, anschaulich geschriebener Leitfaden für alle öffentlichen und privaten Institutionen, zur grundlegenden Vorbereitung und Reaktion auf Cyberangriffe.

Er beschreibt sechs große Themenfelder, die grob der bekannten Einteilung in Govern – Prevent – Detect – Respond zuordenbar sind:

- Verantwortung des Managements – mit klarer Zuweisung der Gesamtverantwortung und einer Reihe von Fragen, die zur Einschätzung des Status Quo bezüglich Cybersicherheit dienen
- Grundlegende technische Maßnahmen – eine Art „Top 10“ wie Software laufend zu aktualisieren, Netzwerke zu segmentieren etc. (s. Anhang 0)
- Bedeutung des Mitarbeiterverhaltens
- Empfehlungen zu Logging und Detektion
- Vorbereitung auf Sicherheitsvorfälle und Notfallszenarien
- Empfehlungen zum Testen der Sicherheitsmaßnahmen, insbesondere Penetration Testing.

Die dänische Publikation ist ein sehr gut geschriebener, eigenständiger Ansatz für den Einstieg in das Thema, im Einklang mit diversen anderen Empfehlungen. Grundlegend neue Aspekte bringt er nicht. Weiterführende Links führen zu Material auf Dänisch und verlinken zu den australischen und kanadischen Ansätzen.

4.19.9 Griechenland: Cybersecurity Handbook

Das griechische „Cyber Security Handbook“ [93] ist ein eigenständiger Ansatz mit „best practices“ für den öffentlichen Sektor sowie mittlere und private große Unternehmen, auf übersichtlichen 76 Seiten.

Es ist in zwei Teile gegliedert:

- Die Einführung
  - empfiehlt Defense-in-depth und Zero-Trust-Architecture als Design-Prinzipien
  - skizziert den Aufbau eines Risikomanagements.
- Der Hauptteil enthält eine Sammlung von 18 „best practices“ mit insgesamt 180 untergeordneten „sub-controls“. Diese decken bekannte Themen wie Inventarisierung, sichere Konfiguration von Endgeräten etc. ab.

Beachtenswert ist, neben den üblichen Controls Design-Prinzipien für sichere Architekturen von IT-Systemen und -Infrastruktur an den Anfang zu stellen – ein Aspekt, der anderen Ansätzen fehlt.

Daneben decken sich die präsentierten Controls weitgehend mit den bereits diskutierten Ansätzen und sind hier nicht detailliert betrachtet.

4.19.10 Irland: 12 Steps to Cyber Security

Die irischen “12 Steps to Cyber Security” [94] sind ein ungewöhnlicher Ansatz: Ein für 12 Monate angelegter Maßnahmenplan, der mit einer Hauptaktivität je Monat die Widerstandsfähigkeit gegen Cyberangriffe stärken soll – ein „Cyber resilience activity plan“. Es ist ein recht kurzer, allgemein gehaltener Ansatz von nur 20 Seiten Länge und ohne Links zu weiteren Details.

Die 12 Schritte bilden aus anderen Ansätzen bekannte Elemente in einem idealtypischen Ablaufplan ab, z. B. beginnend mit „Establish governance and organisation“ sowie Inventarisierung und Klassifizierung unter dem Titel „Identify what matters most“. Konkrete Maßnahmen sind nicht enthalten nur im 6. Monat sehr allgemein beschriebene „basic protections“ aus fünf Bereichen.

Der Ansatz bietet inhaltlich keine neuen Aspekte und ist aufgrund seiner Kürze und fehlenden Verweisen zu weiterführenden Informationen nicht für eine detaillierte Betrachtung geeignet.

4.19.11 UK: 10 Steps to Cyber Security

Die britischen „10 Steps to Cyber Security" [95] sind eine anschaulich geschriebene, leicht lesbare Tour durch 10 wichtige Themen der Cybersicherheit. Sie richten sich an mittlere bis große Organisationen, die wenigstens eine Person zur Betreuung von Cybersicherheit beauftragt haben.

Sie sind mehr eine Themensammlung als konkreter Ratgeber, da sie recht kurz große aufwändige Themen anreißen wie z. B. die Notwendigkeit eines Risikomanagements als allersten Schritt oder einen Schritt „Protect Data", der u. a. mit Backups, Verschlüsselung von data at rest und data in transit mehrere große Themen enthält. Eine kleine Zahl von Links führt von jeder Seite zu detaillierteren Ratgebern. Alle Schritte sind in Anhang 0 gezeigt.

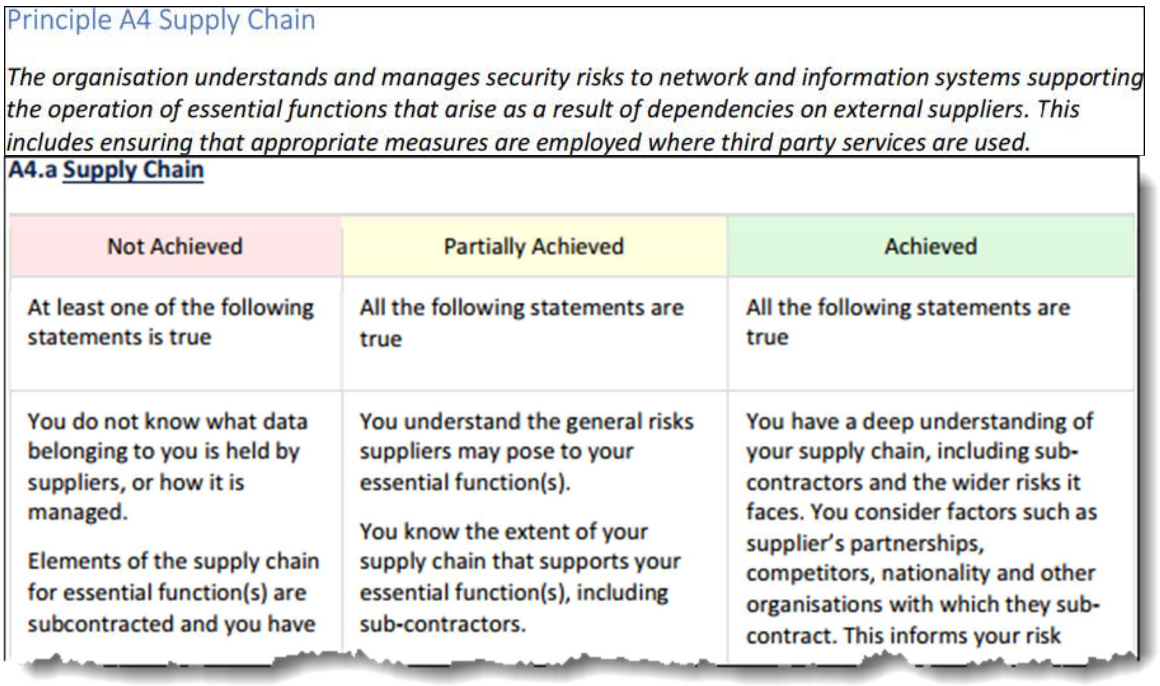
Diese Publikation ist ein sehr guter niederschwelliger Einstieg und Startpunkt, um Aufmerksamkeit für erforderliche Aktivitäten zur Cybersicherheit zu schaffen. Sie ist ausschließlich als Webseite online verfügbar, mit je einer Unterseite für jedes Thema. Als PDF-Dokument gibt es lediglich eine einseitige Grafik, die alle 10 Schritte auflistet.

Insgesamt betrachtet sind die „10 Steps to Cyber Security" aufgrund ihrer geringen inhaltlichen Tiefe nicht für einen Vergleich mit den anderen hier betrachteten Ansätzen geeignet.

4.19.12 UK: Cyber Assessment Framework

Das Cyber Assessment Framework [96] ist ein Leitfaden zur systematischen Bewertung des Umfangs, in dem Cyberrisiken aktiv gesteuert werden – kein ganzheitlicher Ansatz für Informations- oder Cybersicherheit. Die Inhalte sind angelehnt an die Struktur des NIST Cybersecurity Frameworks und der Umfang ist mit 40 Seiten überschaubar.

Es kann eine sinnvolle Alternative sein, um den aktuellen Stand oder den Reifegrad der für Cybersicherheit erforderlichen Prozesse zu bewerten. Er kommt ohne das Abfragen technischer Details aus und kann daher gut auf der Leitungsebene angewendet werden. Er basiert auf „indicators of good practice“ (IGP), d. h. allgemein formulierten Aussagen für verschiedene Erfüllungsgrade einer Anforderung, die eine qualitative Bewertung erlauben. Hier ein Beispiel:



Principle A4 Supply Chain

The organisation understands and manages security risks to network and information systems supporting the operation of essential functions that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.

A4.a Supply Chain

Not Achieved	Partially Achieved	Achieved
At least one of the following statements is true	All the following statements are true	All the following statements are true
You do not know what data belonging to you is held by suppliers, or how it is managed. Elements of the supply chain for essential function(s) are subcontracted and you have	You understand the general risks suppliers may pose to your essential function(s). You know the extent of your supply chain that supports your essential function(s), including sub-contractors.	You have a deep understanding of your supply chain, including sub-contractors and the wider risks it faces. You consider factors such as supplier's partnerships, competitors, nationality and other organisations with which they sub-contract. This informs your risk

Abbildung 39: Beispiele für die „indicators of good practice“ des Cyber Assessment Framework
Quelle: [96, S. 10]

Die Möglichkeit, ohne das Abarbeiten eines Vorgehensmodells und ohne eine Risikoanalyse zu einer trotzdem fundierten Einschätzung des Ist-Zustandes der Cybersicherheit zu kommen, ist eine Besonderheit, die kein anderer der betrachteten Ansätze bietet. Die Nutzung von Indicators of good Practice ist eine sinnvolle Vereinfachung.

4.19.13 UK: Cyber Security Toolkit for Boards

Das „Cyber Security Toolkit for Boards“ [97] ist ein weiteres Dokument mit eigener Zielrichtung: ein Leitfaden für die Management-Ebene, mit allen aus dieser Sicht notwendigen Inhalten für die Implementierung eines ISMS.

Es deckt auf 50 Seiten die von einem ISMS bekannten Themen ab, jeweils mit Schwerpunkt der dafür auf Leitungsebene erforderlichen Aktivitäten und Informationen:

- Integrieren von Cybersicherheit in die Organisation
- Entwickeln einer positiven Unternehmenskultur, die Cybersicherheit fördert
- Fördern von Know-How und Expertise für Cybersicherheit
- Asset Management und Identifizieren der kritischen Assets
- Verstehen der Bedrohungen für Cybersicherheit
- Risikomanagement
- Umsetzen von wirksamen Maßnahmen für Cybersicherheit
- Zusammenarbeit mit Lieferanten und Partnern
- Vorbereiten der Reaktion au Cybersicherheits-Vorfälle

Es ist hier ebenfalls nicht näher betrachtet, da es nicht die Kriterien eines ganzheitlichen Ansatzes im Sinne der Aufgabenstellung erfüllt, kann aber bei beliebigen Projekten zur Stärkung der Cybersicherheit in Organisationen hilfreiche Ergänzung sein.

4.19.14 Kanada: Get cybersafe guide

Der „Get Cyber Safe Guide for Small and Medium Businesses“ [98] ist eine weitere kanadische Veröffentlichung, gerichtet an kleine Unternehmen und legt den Schwerpunkt auf erklärende Texte, weniger vollständige Auflistungen bestimmter Maßnahmen. Dies ist nachvollziehbar, er ist als Teil einer landesweiten Kampagne „Get Cyber Safe“ veröffentlicht, die Aufmerksamkeit für alle Aspekte der Cybersicherheit und viele verschiedene Zielgruppen schaffen soll.

Für diese Zwecke ist er gut geeignet, inhaltlich bringt er keine neuen Erkenntnisse und ist hier nicht genauer betrachtet.

4.19.15 Kanada: Top 10 IT Security Actions

Kanadas “Top 10 IT security actions” [91] sind ein pragmatischer, kurzer Leitfaden für Organisationen, um gezielt mit dem Internet verbundene Netzwerke und Informationen zu schützen.

Sie sind eine reine Maßnahmensammlung von grundlegenden Sicherheitsmaßnahmen mit Links zu weiterführenden Dokumenten, wobei nur für sechs der zehn Maßnahmen ein genau passendes weiterführendes Dokument existiert.

Inhaltlich bringen sie keine neuen Aspekte, sondern sammeln bekannte grundlegende einfache Sicherungen wie das laufende Aktualisieren von Systemen und Applikationen, bewusste Kontrolle administrativer Privilegien einschließlich least privilege und Mehr-Faktor-Authentifizierung, aber auch in der Umsetzung aufwändigere wie die generelle Anforderung nach Systemhärtung und Netzwerksegmentierung in Abhängigkeit vom Schutzbedarf der Informationen. Anhang 0 zeigt alle Maßnahmen.

Die Top 10 IT security actions sind ein sinnvoller kurzer Leitfaden mit Links zu gut geschriebenen weiterführenden Dokumenten, aber ohne neue Erkenntnisse im Sinne der Aufgabenstellung und gegenüber den bereits vorgestellten Ansätzen.

5 Vergleichende Betrachtung

5.1 International dominierende Standards und Bedeutung des IT-Grundschutzes

Mit allen betrachteten achteten Ansätzen zeigt sich eine klare Dominanz von zwei maßgeblichen Standards derart, dass nationale Ansätze sie übernehmen oder als Basis für abgewandelte Fassungen verwenden:

- **ISO/IEC 27001** zum Aufbau eines ISMS für Informationssicherheit und
- **NIST Cybersecurity Framework** für Cybersicherheit.

Daneben existieren einzelne eigenständige Ansätze, von denen vor allem die aus Australien, Belgien und Saudi-Arabien hervorzuheben sind.

Zu dem Aufbau eines ISMS ist die ISO/IEC 27001, die diesen Begriff geprägt hat, gleichzeitig der einzige maßgebliche Standard; es existieren Umsetzungshilfen und leichte Varianten, aber keine grundsätzlich abweichenden oder konkurrierenden Standards.

Der **IT-Grundschutz** hat kaum internationale Resonanz als Umsetzungshilfe oder systematische Vorgehensweise zur ISO/IEC 27001 gefunden. Er wird wenig zitiert und es gibt mit Estland nur einen Fall, in dem ein anderes Land den IT-Grundschutz übernommen hat – und auch nur teilweise das Grundschutz-Kompendium, nicht die Grundschutz-Methodik. Das österreichische Informationssicherheitshandbuch ist unverkennbar sehr stark vom IT-Grundschutz beeinflusst, in seiner Darstellungsform jedoch so eigenständig und ebenfalls ohne die ausführliche Methodik des deutschen IT-Grundschutzes, dass er als verwandter Ansatz, nicht als Adoption einzustufen ist. Der Schweizer IT-Grundschutz suggeriert aufgrund der Namensgleichheit eine enge Verwandtschaft, die nicht gegeben ist.

Eine notwendige Voraussetzung für internationale Verbreitung in Form einer englischsprachigen Übersetzung des IT-Grundschutzes wäre seit Jahren gegeben [99]; auch der bis 2017 gültige Standard 100-2 war seit 2008 auf Englisch verfügbar [32].

Die Anzahl von Google-Suchergebnissen stützen diese Aussage und zeigen zudem eine klar überlegene Popularität von ISO/IEC 27001 gegenüber NIST sowie eine verschwindend geringe Anzahl von Treffern für die vom BSI verwendete Bezeichnung der englischen Übersetzung. Google hat die Anzeige der Anzahl von Suchergebnissen ist im Laufe des Jahres 2023 deaktiviert und zudem ist sie mit Vorsicht zu genießen, da ihre Ermittlung nicht transparent ist und ihre Zuverlässigkeit nicht validiert werden kann. Die Unterschiede sind jedoch so erheblich, dass sie hier trotzdem als unterstützender Indikator dient (zugehörige Screenshots aus 2023 siehe Anhang 0):

Suchbegriff	**Anzahl Suchergebnisse**
ISO/IEC 27001	113.000.000
NIST Cybersecurity Framework	6.380.000
IT-Grundschutz	511.000
BSI „IT Grundschutz Methodology“	1.600
„IT-Grundschutz Compendium“	1.480

Tabelle 6: Anzahl von Google-Suchergebnissen für ISO/IEC 27001, NIST CSF und IT-Grundschutz
Quelle: eigene Recherche und Darstellung

Ein anderer Indikator für die Verbreitung ist die Anzahl der Zertifizierungen, die mangels einer Zertifizierungsmöglichkeit für das NIST CSF nur für ISO/IEC 27001 und den IT-Grundschutz verfügbar sind. Die ISO hat per Ende 2022 die Anzahl der erteilten Zertifikate veröffentlicht [100], vom BSI gibt es eine aktuelle und vollständige Liste aktuell gültiger Zertifizierungen [101]. Die veröffentlichten Zahlen sind:

Art der Zertifizierung	**Anzahl**
ISO/IEC 27001 weltweit (Ende 2022)	71.549
ISO/IEC 27001 in Deutschland (Ende 2022)	1.595
ISO 27001 auf Basis von IT-Grundschutz (Jan. 2024)	151

Tabelle 7: Anzahl Zertifizierungen nach ISO/IEC 27001 und IT-Grundschutz
Quelle: [100] [101]

5.2 Einordnung des IT-Grundschutzes im internationalen Vergleich

Der deutsche IT-Grundschutz hat eine Sonderstellung, es existiert kein vergleichbarer, derart umfangreicher und systematischer Ansatz zur Umsetzung eines ISMS, insbesondere nicht bezüglich seiner wesentlichen Merkmale:

- einer auf ISO/IEC 27001 basierenden ausführlichen Methodik und
- den in Bausteinen organisierten umfangreichen Sicherheitsmaßnahmen.

Bezüglich des dritten wesentlichen Merkmals, der im IT-Grundschutz enthaltenen standardisierten Risikoanalyse existiert kein vergleichbarer Ansatz f*ür Informationssicherheit*. Mit Blick auf Cybersicherheit haben Belgien und Australien eine standardisierte Risikobewertung, basierend auf beobachteten realen Cyberattacken vorgenommen und für eine risikobasierte Auswahl von Sicherheitsmaßnahmen verwendet Zudem ist davon auszugehen, dass bei allen für Cybersicherheit zuständigen Behörden entsprechende Abwägungen in die Auswahl empfohlener „Top-Maßnahmen“ eingeflossen sind, auch wenn es nicht explizit erwähnt und detailliert dokumentiert ist wie in Belgien.

Der Bedarf an konkretisierenden Umsetzungshilfen zur konkreten Anwendung auf einzelne Organisationen ist offensichtlich, beim NIST CSF noch mehr als bei ISO/IEC 27001, da die vom NIST CSF referenzierten Controls des NIST SP 800-53 trotz ihres enormen Umfangs sehr generisch formuliert sind. Von daher zielt der IT-Grundschutz in eine vorhandene große und kaum besetzte Lücke.

5.3 ISO/IEC 27001 vs. NIST Cybersecurity Framework

Bei diesen beiden dominierenden Standards ist eine **Koexistenz** zu erwarten. Sie sind zunächst in ihrem Anwendungsbereich und ihrer Zielstellung ausreichend voneinander abgegrenzt:

- Informationssicherheit bei ISO/IEC 27001 gegenüber Cybersecurity im NIST CSF sowie
- systematischer Ansatz eines Managementsystems bei ISO/IEC 27001 gegenüber einem Fokus auf Sicherheitsmaßnahmen („Controls“) als Teil eines separaten Risikomanagements bei NIST CSF.

In den ISO-Publikationen ist zudem ein langfristiges Nebeneinander durch die anscheinend bislang wenig beachteten eigenständigen Dokumente ISO/IEC 271xx zur Cybersicherheit verankert (siehe 3.3). Sie grenzen Cybersicherheit als Teilbereich der Informationssicherheit von ihr ab und definieren für „Cyber Security Frameworks“ eine Standardstruktur, die wiederum genau den Inhalten des NIST CSF entspricht. Die Weiterentwicklung von ISO/IEC 27001 wird daran nichts ändern; ISO/IEC 27001 bleibt der Kern und in seinen Inhalten stabil, sie wird mit weiteren Bausteinen erweitert, z. B. für Internet of Things oder branchenspezifische Standards [6].

Damit integriert ISO/IEC de facto die Inhalte des NIST CSF als eigenständiges, auf Cybersicherheit fokussiertes Modell und lässt gleichzeitig Wege für weitere Ansätze offen, die dann aber mehr die Rolle bekommen, das sehr generische NIST CSF zu konkretisieren als etwas Eigenes zu entwickeln.

Im NIST CSF gab es mit der neuen übergreifenden Funktion „Govern“ in der Version 2.0 einen Schritt in Richtung der ISMS, indem sie die querschnittliche Aufgabe der systematischen Organisation und Integration von Cybersicherheit in das Unternehmen aufwertet.

5.4 Informationssicherheit vs. Cybersicherheit

Das Begriffspaar Informationssicherheit und Cybersicherheit steht für zwei unterschiedliche Ausrichtungen, die die beiden dominierenden Standards ISO/IEC 27001 und NIST CSF mit sich bringen und die auch bei einem Blick auf alle verglichenen Ansätze gemeinsam klar erkennbar ist, siehe auch die einleitende Grafik in 4.1.

Dabei sind es nur die ISO/IEC 27001 und der IT-Grundschutz sowie deren wenige verwandte Ansätze, die für Informationssicherheit stehen; alle anderen sind auf Cybersicherheit ausgerichtet. Auch ist auffällig, dass fast alle dafür zuständigen nationalen Behörden den Begriff „Cyber“ in ihrer Bezeichnung tragen. „Cybersecurity“ ist außerhalb der Veröffentlichungen zu ISMS der dominierende Begriff; „IT-Sicherheit“ oder das englische „IT security“ spielen kaum eine Rolle.

Das ist offenbar zum einen historisch bedingt; sowohl ISO/IEC 27001 als auch der IT-Grundschutz haben ihren Ursprung in den 1990er Jahren, als die Vernetzung und insbesondere das Internet eine untergeordnete, mit 2024 nicht vergleichbare und Rolle spielten (s. auch 4.3.2). Zu dieser Zeit spielte der Begriff „cybersecurity“ im englischen Sprachraum praktisch noch keine Rolle und die Risiken aufgrund der heute omnipräsenten Vernetzung waren noch vernachlässigbar. Diesen Fokus hat der IT-Grundschutz beibehalten.

Zum anderen ist es in Übereinstimmung mit der bei der Erläuterung der Grundbegriffe gezeigten Besonderheit Deutschlands, dass die Begriffe „IT-Sicherheit“ und „Informationssicherheit“ wesentlich häufiger sind als „Cybersicherheit“ oder „cybersecurity“ (siehe 3.1).

Das Fehlen eines etablierten, ganzheitlichen und klar auf Cybersecurity fokussierten Ansatzes ist eine Lücke im IT-Grundschutz bzw. alternativen Veröffentlichungen des BSI. Die Konzentration auf Cybersecurity wäre risikoadäquat – wie einheitlich von allen betrachteten Ansätzen gefordert.

Eine Integration mit dem IT-Grundschutz wäre naheliegend und erstrebenswert, ist aber vermutlich aufgrund der organisatorischen Trennung im BSI (siehe 4.12) und bisher eigenständigen Angebote der Allianz der Cybersicherheit nicht zu erwarten.

Das australische Information Security Manual und die damit verknüpften „Strategies to mitigate Cyber Security Incidents“ könnten als Vorbild dienen. Ein Vorgehen gegen Risiken für die Cybersicherheit sollte möglich sein, ohne das vollständige umfangreichere Vorgehen für Informationssicherheit und ein vollständiges ISMS zu durchlaufen.

5.5 Vergleich der Vorgehensweisen

Im Umfang ist die Methodik des IT-Grundschutzes mit Abstand am größten und der Vergleich mit anderen Ansätzen stützt die bereits in Abschnitt 4.3.7 formulierten kritischen Gedanken:

- Die beiden dem deutschen Grundschutz am nächsten stehenden Ansätze aus Estland und Österreich übernehmen nicht die umfangreiche Methodik (siehe Abschnitt 4.6.2 und 4.4.2).
- Kein anderer Ansatz formuliert eine derart detaillierte und ausführliche Vorgehensweise.

Eine wie im Grundschutz enthaltene standardisierte Risikoanalyse ist in Bezug auf Informationssicherheit einzigartig, nicht bezüglich Cybersicherheit.

Die anderen Hauptelemente der IT-Grundschutz-Methodik sind – explizit formuliert oder implizit leicht ableitbar – recht einheitlich und in vielen anderen Ansätzen ebenfalls vertreten. Hierzu zeigt die folgende Tabelle die Zuordnung, unter welchen beispielhaften anderen Begriffen vergleichbare Schritte in anderen Ländern auftauchen:

<table>
<tr><th>Schritt in der Methodik der Standardabsicherung</th><th>vergleichbare generische Anforderung</th></tr>
<tr><td>Initiierung des Sicherheitsprozesses</td><td>Management support
information security policy
Sicherheitsziele
security organization</td></tr>
<tr><td>Strukturanalyse</td><td>Inventarisierung</td></tr>
<tr><td>Schutzbedarfsfeststellung</td><td>Kategorisierung von Assets
„Security categorization“ (USA)</td></tr>
<tr><td>Modellierung</td><td rowspan="3">• risikobasierte Auswahl von Sicherheitsmaßnahmen
• Gap-Analyse
• Definition von „control baselines“</td></tr>
<tr><td>IT-Grundschutz-Check</td></tr>
<tr><td>Risikoanalyse</td></tr>
<tr><td>Maßnahmenplan und Umsetzung</td><td>Action plan</td></tr>
</table>

Tabelle 8: Schritte der IT-Grundschutz-Methodik und vergleichbare Begriffe in anderen Ansätzen
Quelle: Eigene Darstellung

Daraus lässt sich eine konkrete Verbesserungsmöglichkeit für den IT-Grundschutz ableiten: eine deutliche Verkürzung der Beschreibung der IT-Grundschutz-Methodik. Abschnitt 4.3.7 hatte bereits eine Zusammenlegung der Standards 200-1 und 200-2 und die Bereinigung begrifflicher Unschärfen und Redundanzen vorgeschlagen. Zusätzlich kann die Darstellung wesentlich kompakter werden, wenn sie die wesentlichen Kernpunkte *ergebnisorientiert* darstellt, in Anlehnung an die „outcome based“ Formulierung z. B. in den USA. Das würde eine sehr kompakte Definition von zu erreichenden Zielen liefern und ausführliche Erläuterungen können wie bisher als nicht verpflichtende Empfehlungen hinzutreten; für die Anwender, die sie gerne in Anspruch nehmen möchten.

Ein **risikobasiertes Vorgehen** ist die große Gemeinsamkeit aller betrachteten Ansätze. Gleichzeitig ist es auch eine Herausforderung für die praktische Umsetzung. Das Ableiten von konkreten Gefährdungen und mehr noch die fundierte Beurteilung von Eintrittswahrscheinlichkeiten und möglichen Auswirkungen haben einen großen Ermessensspielraum und Unsicherheiten. Bei den meisten Ansätzen fehlen aber konkrete Vorgaben und Hilfestellungen dafür, wie man sie sich von staatlichen Stellen wünschen würde, bei denen in nationalen Zentren entsprechende Informationen über Cyberattacken zusammenlaufen. Hier sind der belgische und australische Ansatz vorbildlich. Dem deutschen IT-Grundschutz fehlt mit seiner breiten Sicht auf Informationssicherheit und der Verwendung der G 0-Gefährdungen ein Gegenstück.

Eine für Cyberrisiken sinnvolle Variante ist das im israelischen Ansatz aber auch von der deutschen Allianz für Cybersicherheit vorgeschlagene Modell, Risiken und Schutzbedarf als „exposure“ anhand der Verbindung mit unsicheren Netzen und insbesondere dem Internet zu kategorisieren und daraus das erforderliche Niveau an Schutzmaßnahmen abzuleiten. Eine Integration von Cyberrisiken in den IT-Grundschutz wäre wünschenswert.

5.6 Breite der Anwendbarkeit

Die Anwendbarkeit des IT-Grundschutzes auf Organisationen jeder Art und Größe ist für kleinere Organisationen nicht gegeben (siehe 4.3.7). Eine ergebnisorientierte Formulierung von Maßnahmen, ggf. mit Optionen für unterschiedliche Unternehmensgrößen könnte dieses Defizit beheben.

Ein anderer Blick auf breite Anwendbarkeit ist die Einstiegshürde und der Aufwand für Organisationen, deren Bemühungen um Informations- oder Cybersicherheit am Anfang stehen.

Zum Einstieg in die Informations- oder Cybersicherheit wäre eine Vereinfachung über die Basisabsicherung hinaus möglich. Diese ist zweifellos eine sinnvolle Abkürzung der Standardabsicherung, beinhaltet aber immer noch die Grundschutz-Methodik mit Modellierung und Grundschutz-Checks. Für eine grundlegende Absicherung ist eine direkte Empfehlung und Umsetzung von Maßnahmen möglich und mit weniger Aufwand verbunden.

Die weitere Vereinfachung mit dem „Weg in die Basis-Absicherung“ ist auch keine optimale allgemeingültige Lösung, sie ist entworfen für Kommunalverwaltungen.

Zudem ist gerade beim Einstieg und für ein grundlegendes Sicherheitsniveau eine Fokussierung auf Cybersicherheit sinnvoll. Diese ist weder bei der Basisabsicherung noch dem „Weg in die Basisabsicherung“ gegeben.

Die britischen „Cyber Essentials“ sind ein vorbildliches Beispiel hierfür aufgrund ihrer Verbindung mit einem einfachen Online-Tool, anschaulichen zusätzlichen Hilfen und niedrigschwelligen Zertifizierungsmöglichkeiten zur Überprüfung der Wirksamkeit.

Die deutsche Richtlinie VdS 10000 ist ein weiteres Vorbild für die Anpassung an kleine und mittlere Organisationen.

Die Festlegung eines solchen Programms anhand einer Teilmenge von Grundschutz-Anforderungen könnte Kompatibilität zum vollständigen IT-Grundschutz wahren.

5.7 Sicherheitsmaßnahmen

5.7.1 Inhaltlicher Vergleich

Ein Vergleich der in den betrachteten Ansätzen empfohlenen Sicherheitsmaßnahmen bezüglich ihrer inhaltlichen Breite, d. h. ob es Unterschiede gibt, welche Themen und Aspekte abgedeckt werden oder nicht, ist nicht aussagekräftig zu leisten. Abgesehen vom erheblichen Umfang, dessen Betrachtung den Rahmen dieser Arbeit sprengen würde, ist es nicht aussichtsreich, die unterschiedlich gegliederten und dadurch schwer vergleichbaren Maßnahmenkataloge einander gegenüberzustellen.

Es gibt diverse Ansätze für ein Mapping untereinander, diese sind jedoch nicht aussagekräftig, was hier zwei Beispiele veranschaulichen sollen:

- Ein Mapping zwischen ISO/IEC 27001 dem IT-Grundschutz ist vom BSI verfügbar [102]. Ein inhaltlicher Vergleich ist aufgrund des erheblich unterschiedlichen Umfangs von ISO/IEC 27001 und dem IT-Grundschutz nicht sinnvoll. Die um ein Vielfaches ausführlicheren und detaillierteren Ausführungen in den BSI-Standards und dem Grundschutz-Kompendium führen die knappen ISMS-Anforderungen und in je einem Satz beschriebenen Controls des Annex A weiter aus.
- Ein Mapping zwischen ISO/IEC 27001 und NIST SP 800-53 ist ebenfalls verfügbar [103], in diesem Fall aber wegen der vollständig unterschiedlichen Gliederungen nicht brauchbar.
  Nur ein Beispiel von vielen hierzu: A.8.1 der ISO/IEC 27001 bezieht sich auf User endpoint devices und die genannte Mapping-Tabelle verweist auf zwei Controls AC-11 „Device lock“ und AC-19 „Access control for mobile devices“. Die ISO/IEC 27002 enthält aber noch mehr, z. B. Verschlüsselung, Beschränkung von Software-Installation – das Mapping ist ungenau. Es kann auch nicht zufriedenstellend funktionieren, da die NIST SP-800-53 ihre Controls nicht nach Gerätetypen gegliedert hat.

Weitergehende Bemühungen um ein Mapping z. B. vom IT-Grundschutz zu NIST SP-800-53 werden daher nicht versucht und versprechen keine sinnvollen Erkenntnisse, selbst wenn man den Aufwand dafür betreiben würde.

Wichtiger sind bei der Betrachtung der Sicherheitsmaßnahmen andere Aspekte, die in die Beschreibungen der einzelnen Ansätze geflossen sind:

- inhaltliche Breite und Tiefe der Maßnahmen
- ihr Aufwand zur Ausgestaltung und Interpretation.

5.7.2 Formulierung und Aufbereitung von Sicherheitsmaßnahmen

Hier ist das australische Information Security Manual vorbildlich, das drei wesentliche Verbesserungen bringt:

- Sicherheitsmaßnahmen („Controls“) sind in kurzer, nachprüfbarer Form mit ggf. erläuterndem Text verbunden. Das verbindet die praktische Notwendigkeit zur einfachen systematischen Nachverfolgung mit erläuternder Umsetzungshilfe.
- Der Katalog von Sicherheitsmaßnahmen ist so aufbereitet, dass er sich in großen Teilen direkt als Vorlage für Vorgabedokumente verwenden lässt.
- Jede einzelne Maßnahme hat eine Versionierung und Datum einer eventuellen Aktualisierung. Dies ermöglicht eine fortlaufende Aktualisierung, zeitgemäß veröffentlicht über eine Webseite und mit einem einfachen Tool zur Selektion von Änderungen, falls nötig. Vollständige Veröffentlichungen in Textform sind trotzdem verfügbar, mit beliebigen inkrementellen Updates.

5.8 Vorgabedokumente

Die Erstellung von Vorgabedokumenten, üblicherweise als Richtlinie im Deutschen und „policy“ oder „topic specific policy“ ist bei allen betrachteten Ansätzen mit Aufwand verbunden und bei fast allen nicht mit konkreten Hilfestellungen als Teil eines Vorgehensmodells unterstützt.

Ausnahmen bilden:

- das australische Information Security Manual, das thematisch in „Guidelines“ bezeichneten Kapiteln strukturiert ist, die sich jeweils als Ausgangspunkt für Richtlinien verwenden lassen

- der saudi-arabische Ansatz, der einen umfangreichen Satz von „Policies“ und „Procedures“ bereitstellt.

Zumindest eine mögliche Gliederung von Vorgabedokumenten, an der Organisationen sich orientieren können, finden sich in

- dem amerikanischen Standard NIST SP 800-53, der in jeder seiner 20 Control Families als erste Control einen Eintrag „Policy and Procedures“ hat (siehe Abschnitt 4.10.2 für eine Liste)
- der ISO/IEC 27002 in Form der dort empfohlenen 17 „topic specific policies“ (siehe Anhang 8.3 für eine Liste).

Der IT-Grundschutz hat eine sehr große Anzahl von Anforderungen an Vorgabedokumente, die bei genauer Befolgung auch für große Organisationen nur schwer zu leisten ist und in der Praxis ein Zusammenlegen ähnlicher Dokumente erfordert (siehe Abschnitt 4.3.5 für eine Zusammenfassung, Anhang 0 für eine Liste).

6 Gegenüberstellung des IT-Grundschutzes mit MITRE ATT&CK und D3FEND

6.1 IT-Grundschutz und MITRE ATT&CK

6.1.1 Charakterisierung von MITRE ATT&CK

Hintergrund und Zielsetzung

MITRE ATT&CK ist eine Wissenssammlung über und eine Modellierung des Angreiferverhaltens bei Cyberattacken [104]. Entwickelt hat dieses Modell The MITRE Corporation, eine seit 1958 bestehende amerikanische Gesellschaft, die im Auftrag der Vereinigten Staaten eine Reihe von Forschungsinstituten unterhält und im Zusammenhang mit IT-Sicherheit vor allem durch die „Common Vulnerabilities and Exposures“ (CVEs) bekannt ist [105]. ATT&CK steht für „Adversarial Tactics, Techniques and Common Knowledge” und damit für die im Anschluss erläuterten Grundbegriffe des ATT&CK-Modells.

ATT&CK versteht sich nicht als vollständige Sammlung aller möglichen Angriffsvektoren und auch nicht als Sammlung möglicher Bedrohungen, die wie eine Checkliste vollständig bekämpft werden sollen – „coverage of every ATT&CK technique is unrealistic“ [104, S. 4].

Struktur von MITRE ATT&CK

Kernstück von MITRE ATT&CK ist die ATT&CK Matrix, die folgende Elemente enthält:

- **Tactics:** Kurzfristige Ziele, die ein Angreifer während einer Attacke erreichen möchte, z. B. erstmaligen Zugang zu einem System bekommen („Initial Access“) oder höhere Zugriffsrechte zu erhalten („Privilege Escalation“). ATT&CK hat 14 solcher Taktiken identifiziert [106], eine vollständige Liste ist im Anhang 0.
- **Techniques:** Konkrete Aktivitäten, die ein Angreifer ausführt, um ein taktisches Ziel zu erreichen. Für jede Taktik kann es eine Vielzahl von

Techniken geben, insgesamt hat ATT&CK 202 Techniken mit 435 Varianten („Sub-techniques“) identifiziert [107].

Die ATT&CK Matrix existiert in drei Varianten, „Technology Domains“ genannt:

- Enterprise für Organisationen und dort dominierende Technologien: Windows, macOS, Linux, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network, Containers.
- Mobile für Android und iOS-Systeme
- ICS für industrielle Steuerungssysteme.

Die weitere Betrachtung bezieht sich nur auf die Variante Enterprise.

Nachfolgend ein Ausschnitt der Matrix für die Taktik „Initial Access“, für eine vollständige Wiedergabe hier ist sie zu groß:

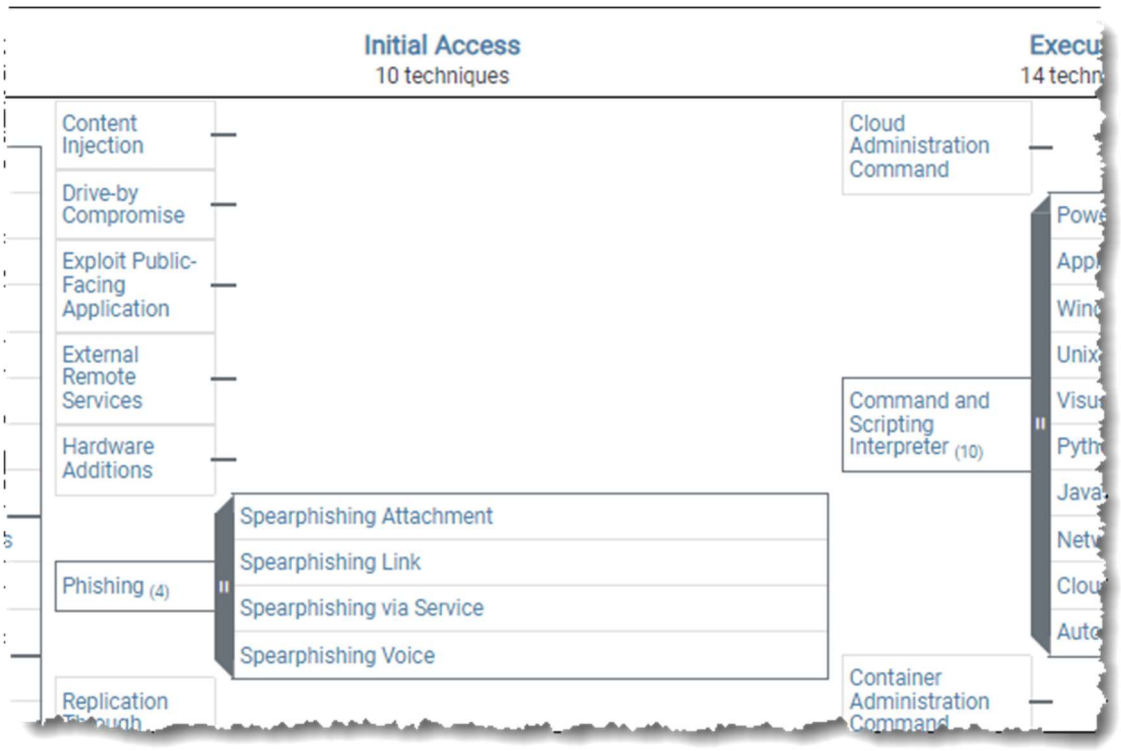


Abbildung 40: Ausschnitt aus MITRE ATT&CK Enterprise Matrix
Quelle: [108].

Das gesamte MITRE ATT&CK-Modell ist größer, berücksichtigt auch Informationen über Angreifer, mögliche Detektions- und Abwehrmaßnahmen:

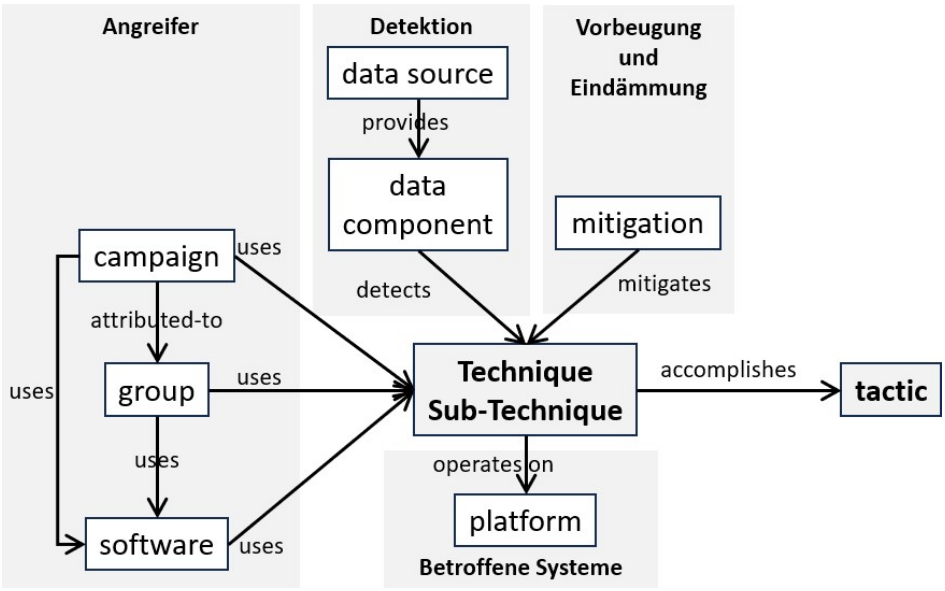


Abbildung 41: Struktur des MITRE ATT&CK-Modells
Quelle: Eigene Darstellung, basierend auf [109]

- In der Mitte stehen die erläuterten Aktivitäten von Angreifern – **Techniques und Sub-Techniques** – mit ihren taktischen Zielen rechts daneben.
- Links sind Informationen zu **Angreifern**, soweit bekannt: Angreifergruppen (groups) und ihre verwendeten Tools (software) sowie eine Gruppierung von offenbar zusammenhängenden Angriffsaktivitäten zu sog, „campaigns“, z. B. alle 2022 gegen die ukrainische Stromversorgung gerichteten Aktivitäten.
- Informationen zur möglichen **Detektion** sind links über der Mitte gezeigt und geben dafür konkrete technische Hinweise: Welche Datenquellen („data sources“, z. B. Active Directory, Application Logs) an welcher Stelle („data component“, z. B. AD Credential Request, AD Object Access) Hinweise auf die Anwendung einer Angriffstechnik geben
- Informationen zur möglichen **Vorbeugung oder Eindämmung („mitigation“)** stehen rechts über der Mitte, Details zu ihnen folgen weiter unten.

Diese Grafik entspricht einem für bessere Anschaulichkeit vereinfachten ERM-Modell, nach dem alle Daten des MITRE ATT&CK-Modells für Auswertungszwecke in verschiedenen Formaten verfügbar sind, z. B. zur Abfrage mit Python-Tools oder auch in einfachen Excel-Tabellen [110].

6.1.2 Anwendungsmöglichkeiten von MITRE ATT&CK

Die MITRE ATT&CK-Webseite nennt folgende Anwendungsfälle („use cases“) für MITRE ATT&CK, die zunächst keine direkte Verbindung zum IT-Grundschutz und vergleichbaren Ansätzen nahelegen:

- **Detection and Analytics**: Verwendung des ATT&CK-Modells zur Verbesserung konkreter Detektionsmaßnahmen. Ein einfacher Ansatz beginnt mit den oben gezeigten „data sources“; ein Abgleich der in ATT&CK verzeichneten mit den in der Organisation vorhandenen ist leicht möglich, anschließend lassen sich daraus geeignete Detektionsmaßnahmen entwickeln. Ein fortgeschrittenerer Ansatz beginnt mit ausgewählten Techniken, recherchiert in MITRE ATT&CK zugehörige mögliche Detektionen und setzt diese in der eigenen Organisation um.
- **Threat Intelligence**: Hierfür lassen sich zum einen aus ATT&CK sehr konkrete potentielle Bedrohungen ableiten, indem Analysten für die jeweilige Organisation relevante und zuvor identifizierte Angreifer recherchieren. Anschließend können gezielt Schutz- und Detektionsmaßnahmen gegen die von ihnen verwendeten Techniken geplant werden. Zum anderen lassen sich aus beobachteten Sicherheitsvorfällen Rückschlüsse auf die zugrundeliegenden Techniken, Taktiken und möglicherweise Angreifer ziehen, was wiederum wertvolle Hilfe für das Ergreifen von Folgemaßnahmen ist.
- **Adversary Emulation and Red Teaming**: Nutzung der in ATT&CK beschriebenen Techniken, um zu testen, ob sie erkannt würden; im einfachsten Fall simulieren dabei Tools die Angriffe von Tools, für fortgeschrittene Tests Red Team-Penetration-Tester.
- **Assessment and Engineering**: Eine schrittweise Bewertung aller in ATT&CK dokumentierten Techniken daraufhin, ob sie entdeckt würden oder nicht. Dabei können risikobasiert bestimmte Techniken bevorzugt validiert werden und anschließend ausgewählte Lücken verkleinert werden.

Alle beschriebenen Anwendungen arbeiten mit den in ATT&CK dokumentierten Informationen – losgelöst von den diversen zuvor beschriebenen Ansätzen für Informationssicherheit bzw. Cybersicherheit und den aus ihnen abgeleiteten

Maßnahmen. Zudem sind sie naturgemäß für Organisationen, die eine bereits bestehende Absicherung haben und mit Hilfe von MITRE ATT&CK gezielte Verbesserungen und sehr fortgeschrittene Analysen vornehmen – und dafür auch entsprechende personelle Ressourcen haben.

6.1.3 Ansatzpunkte für eine Gegenüberstellung mit dem IT-Grundschutz

Eine Gegenüberstellung mit dem IT-Grundschutz oder anderen Ansätzen ist in den beschriebenen publizierten Anwendungsfällen von MITRE ATT&CK nicht vorgesehen und auch in der Literatur nicht zu finden. Er ist offenbar Neuland, soll aber trotzdem versucht werden, da er aus zwei Gründen plausibel scheint:

- Jede in MITRE ATT&CK beschriebene Angriffstechnik ist eine potentielle Bedrohung für Organisationen und damit möglicher Input für Risikoanalysen. Der Gesamtumfang aller über 200 Techniken und ihrer über 400 Abwandlungen ist für eine genaue Risikoanalyse zu umfangreich und zudem hinsichtlich Eintrittswahrscheinlichkeit und möglicher Auswirkungen nicht glaubwürdig zu bewerten. Mit einer sinnvollen Eingrenzung ändert sich jedoch das Bild deutlich:
  - Eine Analyse tatsächlich auftretender Angriffe und Zuordnung zu MITRE ATT&CK-Techniken und den zugehörigen „mitigations“, also Schutzmaßnahmen könnte sehr konkrete Daten über vorherrschende Techniken liefern und Maßnahmen ableiten – risikobasiert, wie von allen Ansätzen gefordert.
  - Gleiches gilt, wenn aufgrund aktueller Bedrohungen von bekannten Angreifern ein Fokus auf bestimmte Techniken zu erwarten ist. Dies ist in hohem Maße praxisrelevant, z. B. russische Angreifer wie APT28, APT29, Cozy Bear u. a. sind über Jahre hinweg aktiv.
- Die in MITRE ATT&CK beschriebenen „mitigations“ sind eine Brücke zu den Schutzmaßnahmen der zuvor beschriebenen ganzheitlichen Ansätze.

Zu dem ersten Punkt existiert eine Untersuchung der mit MITRE verbundenen MITRE Engenuity: *15 der erfassten Techniken decken 90 % der in einer Studie beobachteten realen Angriffe ab, basierend auf 6 Mio. Beobachtungen 2019 – 2021* [58]. Entsprechend wäre auch eine risikobasierte Berücksichtigung

und Priorisierung der relevantesten Sicherheitsmaßnahmen in Standards wie dem IT-Grundschutz möglich.

Die in realen Cyberangriffen verwendeten Techniken zu identifizieren, die ein besonderes hohes Risiko darstellen, wäre eine Aufgabe, für die staatliche CERTs und Cybersicherheits-Behörden prädestiniert sind. Die anschließende Ableitung von Schutz- und Detektionsmaßnahmen aus MITRE ATT&CK wäre naheliegend, da dies ein etabliertes, weithin akzeptiertes Modell ist und kein anderes bekannt ist, das von Angriffstechniken eine Brücke zur Detektion und zu Schutzmaßnahmen schlägt. Entsprechende Aktivitäten und Veröffentlichungen waren jedoch in der Recherche für diese Arbeit nicht zu finden.

Im Ergebnis zeigen sich also zwei durchaus sinnvolle Verbindungen zwischen MITRE ATT&CK und den ganzheitlichen Ansätzen für IT-Sicherheit, die jedoch mehr für die Erstellung dieser Ansätze relevant sind als für die Organisationen, die sie anwenden. Die jeweiligen Behörden für Cybersicherheit könnten also durchaus davon profitieren, damit auch das deutsche BSI.

6.1.4 Gegenüberstellung von Mitigations und Sicherheitsmaßnahmen

Übersicht der Mitigations

Die Anzahl der Mitigations in MITRE ATT&CK ist mit 43 überschaubar. Darunter sind technisch orientierte wie z. B. Network Segmentation oder Active Directory Configuration ebenso wie einfache, leicht umsetzbare, z. B. Mehrfaktor-Authentifizierung oder regelmäßige Softwareaktualisierungen. Die vollständige Liste zeigt Anhang 0.

Die aufgrund ihrer geringen Anzahl recht generisch formulierten Mitigations haben für jede Technik, auf die sie Anwendung finden, eine Ausprägung mit einer zugehörigen Beschreibung. Beispiel:

- Eine der 43 Mitigations ist „Application Isolation and Sandboxing."
- Eine der für sie relevanten Angriffstechniken ist "Drive-by Compromise", wobei sich ein Angreifer alleine durch den Aufruf einer manipulierten Webseite sich einen Zugang zum angegriffenen System verschafft.

- Die konkrete Ausprägung der genannten Mitigation für diese Technik ist dann „Browser sandboxing“. Für andere Anwendungen gibt es entsprechend andere Wege, sie vom Rest eines Systems zu isolieren wie z. B. Virtualisierung.

Mit ihrer Anwendung auf die zahlreichen Techniken ergibt sich eine sehr große Zahl von Ausprägungen – insgesamt 1200 Zuordnungen von Mitigations zu Techniques, darunter ca. 800 verschiedene Ausprägungen, wie eine Auswertung der von MITRE in Tabellenform bereitgestellten Mitigations zeigt.

Auswahl einer Stichprobe von Techniques und Mitigations

Die für jeden erfolgreichen Angriff erforderliche Taktik „Initial Access“ ist bei MITRE ATT&CK mit 9 Techniken verknüpft, zuzüglich 10 Varianten davon. Für diese überschaubare Teilmenge sollen zugehörige Mitigations einzeln untersucht und auf ihre Übereinstimmung mit dem IT-Grundschutz geprüft werden. Dabei ist kein rein schematischer Vergleich möglich, für einen korrekten Abgleich ist jede Technik und Schutzmaßnahme inhaltlich zu betrachten und zu verstehen, um eine Entsprechung im Grundschutz finden zu können.

Die zur Taktik „Initial Access“ gehörenden Angriffstechniken sind:

ID	name
T1189	Drive-by Compromise
T1190	Exploit Public-Facing Application
T1133	External Remote Services
T1200	Hardware Additions
T1566	Phishing
T1091	Replication Through Removable Media
T1195	Supply Chain Compromise
T1199	Trusted Relationship
T1078	Valid Accounts

Abbildung 42: Mit Taktik „Initial Access“ verknüpfte Angriffstechniken von MITRE ATT&CK
Quelle: Eigene Auswertung, basierend auf [110]

Gegenüberstellung der Mitigations mit IT-Grundschutz-Anforderungen

Im Ergebnis soll für jede Mitigation eine Bewertung in einer der folgenden Kategorien erfolgen:

- **Übereinstimmung**: Mitigation lt. MITRE ATT&CK ist im Grundschutz enthalten
- **ATT&CK konkretisiert IT-Grundschutz**: Mitigation lt. MITRE ATT&CK ist im IT-Grundschutz enthalten, aber ATT&CK enthält zusätzliche und für die praktische Umsetzung hilfreiche Konkretisierungen oder Details
- **IT-Grundschutz konkretisiert ATT&CK**: wie zuvor, aber in umgekehrter Richtung
- **ATT&CK ergänzt IT-Grundschutz**: Mitigation lt. MITRE ATT&CK ist im Grundschutz nicht vorhanden

Das Vorgehen ist an einem ersten Beispiel hier gezeigt, der vollständige Abgleich aller weiteren Fälle ist im Anhang 0 dokumentiert.

Angriffstechnik:	**Drive-by Compromise**
Ziel:	Angreifer bekommt Zugang zu einem System bei einem normalen Webseiten-Besuch eines Users mit Browser; ohne dass ein User Dateien herunterlädt
Funktionsweise:	Erforderlicher Schadcode kann auf verschiedene Weise auch auf an sich vertrauenswürdige Webseiten gelangen, z. B. durch • Angriffe auf den zugehörigen Webserver • Manipulation von Skript-Dateien, die eine Webseite nachlädt, • in bezahlter Werbung platzierter Schadcode • Cross-Site Scripting Beim Aufruf einer Webseite läuft dann ein Skript ab, das nach Browser- und Plug-in-Versionen mit Schwachstellen sucht und ggf. zugehörigen Exploit-Code nachlädt und ausführt. Anschließend kann der Angreifer Code auf dem angegriffenen Endgerät ausführen – sofern nicht andere Schutzmaßnahmen dies verhindern. Über das kompromittierte Endgerät besteht möglicherweise direkter Zugriff auf das interne Netz, eine Abschirmung mit einer DMZ würde umgangen.

Angriffstechnik:	**Drive-by Compromise**
Mitigation:	**Application Isolation and Sandboxing**
MITRE-Beschreibung:	Browser sandboxing kann Auswirkungen der Code-Ausführung verhindern, allerdings können „Sandbox escapes“ möglich sein. Alternativ andere Virtualisierungstechniken oder „application microsegmentation“; dann sind zwar noch weitere exploits denkbar (virrtual machine escape), würden aber einen schwierigeren mehrstufigen Angriff erfordern.
IT-Grundschutz:	APP.1.2.A1: Browser-Sandboxing ist erste Basis-Anforderung, enthält auch Content Security Policy CSP und Same-Origin-Policy → mehr und detaillierter als MITRE APP.1.2.A9: Virtualisierung oder ReCoBS (Remote Controlled Browser System = Browser auf separatem Rechner und Bedienung über Remote Desktop) für erhöhten Schutzbedarf
Bewertung:	IT-Grundschutz konkretisiert MITRE ATT&CK
Mitigation:	**Exploit Protection**
MITRE-Beschreibung:	Nutzung von Schutzmaßnahmen, um Bedingungen zu erkennen und zu stoppen, die Software-Exploits ermöglichen oder auf sie hinweisen, z. B.: • Windows Defender Exploit Guard WDEG; eine Schutzfunktion in Windows 10 an Version 1709 von 2017. Der WDEG enthält Exploit Protection als eine von vier Komponenten. • Control Flow Integrity checking; dies sind Schutzmaßnahmen, die Änderungen im Programmablauf und Manipulation von Sprungadressen verhindern. Es gibt verschiedene Implementationen von Microsoft Control Flow Guard (CFG); dieser muss beim Kompilieren eines Programms eingebunden werden und es scheinen mehrere Techniken zu existieren, ihn zu umgehen.
IT-Grundschutz:	SYS.2.1.A9 fordert die Festlegung einer Sicherheitsrichtlinie für Clients, allerdings ohne jegliche Empfehlung für Konfigurationsdetails SYS.2.2.3 für Windows-Clients enthält keinerlei Hinweise auf Windows-spezifische Konfigurationsdetails. Auch im restlichen Kompendium sind keine Hinweise auf den Windows Defender Exploit Guard WDEG oder CFG.
Bewertung:	MITRE ATT&CK enthält sinnvolle Konkretisierung für IT-Grundschutz

Tabelle 9: Abgleich zweier Mitigations/ aus MITRE ATT&CK mit IT-Grundschutz
Quelle: Eigene Auswertung

Ergebnis der Gegenüberstellung

Eine Auszählung der detaillierten und im Anhang 0 dokumentierten Vergleiche ergibt folgende Zahlen:

Ergebnis	Anzahl	%
Übereinstimmung	15	44 %
ATT&CK konkretisiert Grundschutz	8	24 %
Grundschutz konkretisiert ATT&CK	1	3 %
ATT&CK ergänzt IT-Grundschutz	10	29 %
Summe	**34**	**100 %**

Tabelle 10: Ergebnisse des Abgleichs einer Stichprobe von Mitigations aus MITRE ATT&CK und IT-Grundschutz
Quelle: Eigene Auswertung4

Die betrachtete Stichprobe zeigt, dass ein genauer Abgleich der MITRE ATT&CK Enterprise Mitigations mit den Anforderungen des IT-Grundschutz-Kompendiums durchaus neue Erkenntnisse bringt. Es finden sich sinnvolle zusätzliche Details für vorhandene, allgemeiner formulierte Anforderungen oder Aspekte für zusätzliche Anforderungen – *immerhin bei der Hälfte der untersuchten Stichprobe.*

Da eine risikobasierte Eingrenzung auf besonders relevante Angriffstechniken den Umfang relevanter Techniken und Mitigations sehr stark reduziert (s. 6.1.3), erscheint der skizzierte Ansatz aussichtsreich für eine wirksame Verbesserung im IT-Grundschutz.

6.2 IT-Grundschutz und MITRE D3FEND

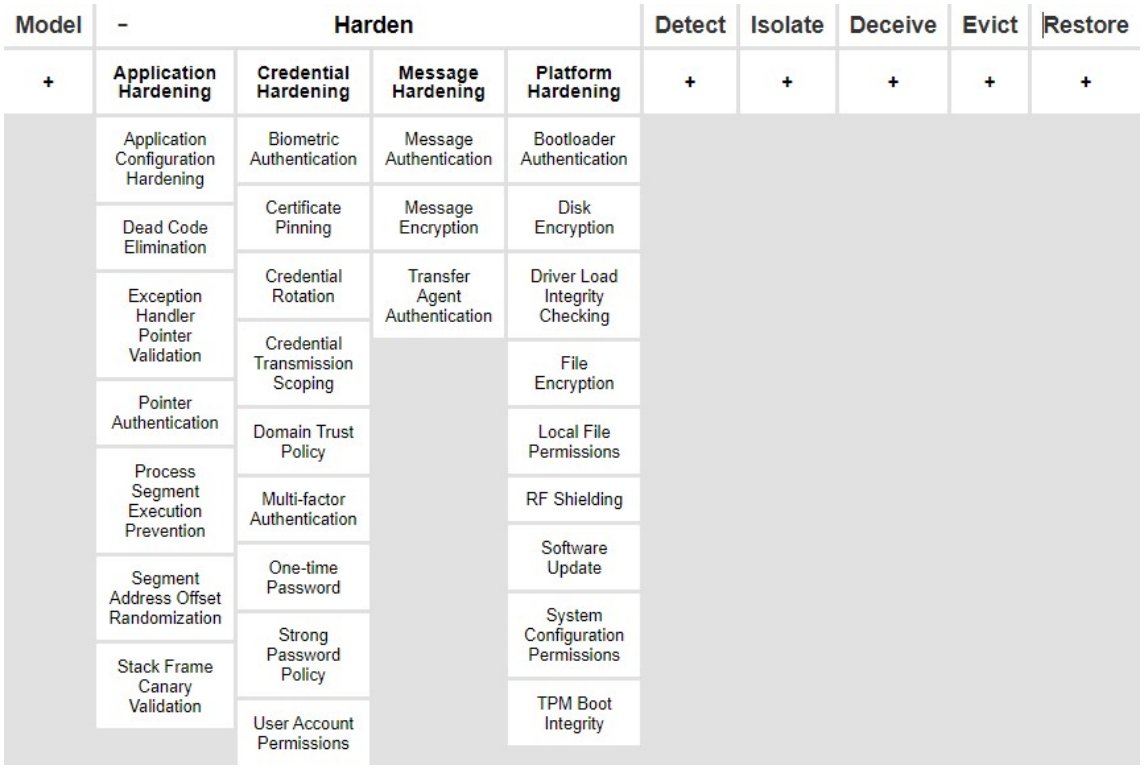
MITRE D3FEND steht für „Detection, Denial and Disruption Framework Empowering Network Defense". Es hat zum Ziel, einen „knowledge graph of cybersecurity countermeasures" zu bilden – Wissen über Sicherheits-maßnahmen zu sammeln und zu ordnen; zu verstehen, wie sie wirken, nicht nur, was sie erreichen [111]. Daneben ist die Definition einer einheitlichen, semantisch klar definierten Terminologie erklärtes Ziel.

Die Ergebnisse des D3FEND-Modells sind in einer Matrix visualisiert, die sehr an die Matrix von ATT&CK-Tactics und -Techniques erinnert. In gleicher Struktur sind hier defensive Techniken gesammelt und einer überschaubaren Zahl von Taktiken zugeordnet, denen sie dienen [112]. Diese Taktiken sind:

Model	Strukturierung und einheitliche modellhafte Beschreibung von Systemen, Akteuren und ihren Aktivitäten sowie aller Beziehungen untereinander
Harden	Techniken, die es Angreifern erschweren, ein Computer-Netzwerk für ihre Zwecke zu missbrauchen („exploit“)
Detect	Zugang von Angreifern zu einem Netzwerk oder ihre Aktivitäten darin erkennen
Isolate	Logische oder physische Barrieren aufbauen, die es erfolgreichen Angreifern erschweren, ihre Angriffe auszuweiten
Deceive	Techniken, um Angreifer täuschen und zu einem dafür vorbereiteten, kontrollierten Teilsystem zu locken
Evict	Angreifer aus einem Computer-Netzwerk entfernen
Restore	Angegriffene Systeme wiederherstellen oder in ihrem Zustand verbessern

Tabelle 11: MITRE D3FEND Tactics
Quelle: [112]

Zu diesen Taktiken beschreibt MITRE D3FEND ca. 180 Techniken mit hohem Abstraktionsgrad – sie sind nicht für eine direkte praktische Umsetzung vorgesehen.



Model	-	Harden			Detect	Isolate	Deceive	Evict	Restore
+	Application Hardening	Credential Hardening	Message Hardening	Platform Hardening	+	+	+	+	+
	Application Configuration Hardening	Biometric Authentication	Message Authentication	Bootloader Authentication					
	Dead Code Elimination	Certificate Pinning	Message Encryption	Disk Encryption					
	Exception Handler Pointer Validation	Credential Rotation	Transfer Agent Authentication	Driver Load Integrity Checking					
	Pointer Authentication	Credential Transmission Scoping		File Encryption					
	Process Segment Execution Prevention	Domain Trust Policy		Local File Permissions					
	Segment Address Offset Randomization	Multi-factor Authentication		RF Shielding					
	Stack Frame Canary Validation	One-time Password		Software Update					
		Strong Password Policy		System Configuration Permissions					
		User Account Permissions		TPM Boot Integrity					

Abbildung 43: Ausschnitt der MITRE D3FEND-Matrix
Quelle: [112]

Die FAQs zu MITRE D3FEND schreiben dazu ausdrücklich, dass das Modell nicht dafür vorgesehen ist, bestimmte Sicherheitsmaßnahmen zu empfehlen, Prioritäten zu definieren oder ihre Wirksamkeit zu beurteilen [113].

Die gezeigte Matrix ist nicht der Hauptbestandteil von D3FEND. Dahinter steht ein komplexeres Modell, eine Ontologie von digitalen Artefakten [111, S. 8]. Digitale Artefakte sind dabei beliebige digitale Objekte von Interesse für Cybersicherheit-Analysen, z. B. Dateien, Netzwerkverkehr, Software mit zahlreichen Unterkategorien – über 600 hat MITRE D3FEND definiert. Diese digitalen Artefakte sind auch die Brücke zu MITRE ATT&CK, da Angriffstechniken ebenfalls mit diesen Artefakten interagieren, z. B. sie verändern. Eine Ontologie stellt netzwerkartige Verbindungen logischer Beziehungen zwischen den Elementen her, anders als eine hierarchische Taxonomie.

Damit hat MITRE D3FEND eine ganz andere Zielrichtung als MITRE ATT&CK, es ist nicht etwa ein inhaltlich auf Abwehrmaßnahmen spezialisiertes Modell mit gleicher Struktur und Praxisnähe, wie der Name alleine vermuten ließe.

Weder aus den von MITRE vorgesehenen Anwendungen für MITRE D3FEND noch aus einem Blick auf seine bislang veröffentlichten Inhalte ergeben sich Ansatzpunkte für eine Gegenüberstellung mit dem IT-Grundschutz oder anderen zuvor beschriebenen Modellen.

6.3 Fazit der Gegenüberstellung des IT-Grundschutzes mit MITRE ATT&CK und D3FENSE

Eine Gegenüberstellung des IT-Grundschutzes mit MITRE ATT&CK hat durchaus vielversprechende Ansätze gezeigt, um Informationen aus MITRE ATT&CK in den IT-Grundschutz – oder andere vergleichbare ganzheitliche Ansätze – zu integrieren:

- Die Details zu Sicherheitsmaßnahmen („mitigations“) aus MITRE ATT&CK lassen können sinnvolle neue Aspekte im IT-Grundschutz ergänzen oder vorhandene Anforderungen hilfreich konkretisieren. Dies war bei der Hälfte einer betrachteten Stichprobe der Fall. Ein solcher Abgleich ist allerdings mühsam und sollte nicht den Anwendern des IT-Grundschutzes überlassen bleiben, sondern idealerweise bereits in seine die Erstellung einfließen.
- Zusammen mit Informationen aus in der Realität beobachteten Cyberattacken ist eine wertvolle Hilfestellung einer überall geforderten risikobasierten Auswahl von Sicherheitsmaßnahmen möglich: Die Identifikation von besonders häufigen Angriffstechniken und dagegen wirksamer Abwehrmaßnahmen.

  Auch dies ist nicht für die Anwender von Standards wie dem IT-Grundschutz zu leisten, kann aber erhebliche Aufwertung und Qualitätsverbesserung bringen, wenn solche Informationen z. B. aus einem staatlichen CERT in die Erstellung der Standards einfließen.
- Für die Detektion von Cyberangriffen enthält der IT-Grundschutz ebenso wie andere betrachtete Ansätze keine detaillierten Empfehlungen. Organisationen, die mit eigenem Personalaufwand ihre Abwehr dafür verbessern möchten, finden in MITRE ATT&CK wertvolle Informationen, die keiner der betrachteten Ansätze in diesem Umfang liefert.

Der Versuch einer Gegenüberstellung des IT-Grundschutzes mit MITRE D3FEND hat sich als nicht fruchtbar erwiesen.

7 Zusammenfassung von Ergebnissen

Dieser Abschnitt stellt thesenartig Aussagen aus anderen Kapiteln zu einer kritischen Würdigung und Diskussion des IT-Grundschutzes sowie einer vergleichenden Betrachtung mit anderen Ansätzen zusammen.

Er ist als Sammlung von Erkenntnissen zu sehen, nicht als konkreter Vorschlag von Verbesserungen und Weiterentwicklungen. Eine Konsolidierung und Übersetzung in konkrete Vorschläge sind hier weder beabsichtigt noch vom Umfang her zu leisten.

Gesamtbewertung

- Der IT-Grundschutz ist einzigartig bezüglich seiner ausführlichen Methodik und umfänglichen, in Bausteinen gegliederten Sammlung von Anforderungen im Grundschutz-Kompendium.
- Er füllt damit eine wichtige Lücke als Umsetzungshilfe für ISO/IEC 27001, wie sie für das amerikanische NIST CSF ebenfalls wünschenswert wäre, aber in allen Recherchen zu dieser Arbeit nicht auffindbar war.
- Im Detail liegt beim IT-Grundschutz erhebliches Verbesserungspotential.
- Die als Ziel angegebene Anwendbarkeit auf Unternehmen beliebiger Art und Größe ist insgesamt kritisch zu sehen und für kleine Unternehmen nicht gegeben (siehe 4.3.7).
- Internationale Resonanz hat der IT-Grundschutz nur sehr wenig gefunden (siehe 5.1).

Informationssicherheit und ISMS vs. Cybersicherheit

- Der IT-Grundschutz steht zusammen mit der ISO/IEC 27001 und wenigen anderen Ansätzen für Informationssicherheit, systematisch umgesetzt mit einem ISMS.

  Die Mehrheit aller gefundenen Ansätze fokussiert auf Cybersicherheit, wo das amerikanische NIST Cybersecurity Framework der dominierende Standard ist (s. 4.1).
- Eine Anwendung des IT-Grundschutzes gezielt für Risiken der Cybersicherheit ist nicht möglich, wäre aber zeitgemäß und risikoadäquat.

- Die in den ISO/IEC-Standards dokumentierte Verbindung zwischen Informations- und Cybersicherheit (siehe 4.11) ist im IT-Grundschutz nicht vorhanden und berücksichtigt.
- Ein ganzheitlicher, systematischer und breit anwendbarer Ansatz für Cybersicherheit fehlt in Deutschland (siehe 4.12)
- Der IT-Grundschutz ist nur sehr lose mit den Aktivitäten des BSI zur Cybersicherheit verbunden und integriert (siehe 4.12)

Vorgehensweise

- Eine risikobasierte Vorgehensweise ist die große Gemeinsamkeit aller betrachteten Ansätze.
- Über weitere Hauptelemente des IT-Grundschutzes – Inventarisierung, Kategorisierung, Definition von Maßnahmen aus vorgegebenen Katalogen und eigener Risikobetrachtung – besteht ebenfalls breiter Konsens.
- Kein anderer Ansatz formuliert eine derart detaillierte, formalisierte und ausführliche Vorgehensweise.
- Eine integrierte Risikoanalyse basierend auf realen Cyberattacken und darauf basierend abgestufte Maßnahmen finden sich in den belgischen Cyber Fundamentals (siehe 4.13) und wäre eine zeitgemäße Bereicherung des risikobasierten Grundschutz-Ansatzes.
- Die australischen Strategien gegen Cyberrisiken sind ein weiterer Ansatz, der gezielt Anwendern die risikobasierte Auswahl abnimmt. Deren Integration in einen umfangreicheren Maßnahmenkatalog ist vorbildlich (siehe 4.16.4).
- Der IT-Grundschutz hätte das Potential, etwas sehr Ähnliches anzubieten, indem er in der Logik der bisher nur mühsam anwendbaren Kreuzreferenztabellen integriert und mit einem simpel zu bedienenden Tool zu unterstützt (siehe 4.16.6).
- Die Beschränkung auf ausgewählte, direkt anwendbare „Top-Maßnahmen“ ist gängig als Vereinfachung oder Einstiegsmodell, im IT-Grundschutz bisher nicht vorhanden. Auch dessen Basisabsicherung ist mit dem zusätzlichen Schritt der Modellierung und Grundschutz-Checks komplexer.

- Sinnvoll abgestufte Maßnahmenpakete finden sich z. B. in Belgien (siehe 4.13) und Singapur (siehe 4.19.2).

Sicherheitsmaßnahmen

- Die Konzentration auf *sicherheitsrelevante* Anforderungen im Grundschutz-Kompendium wäre eine wichtige Verbesserung. Sie ist derzeit nicht gegeben und die laufende Überarbeitung des IT-Grundschutzes scheint sie nicht zu berücksichtigen (siehe 4.3.7 und 0).
- Eine *ergebnisorientierte* Formulierung von Anforderungen im Kompendium würde ebenfalls Vorteile für bessere Anwendbarkeit in beliebigen Organisationen bringen (siehe 4.3.7, 4.10.3). Sie sollte mit der Nennung möglicher Optionen und Alternativen zur Umsetzung einhergehen.
- Methodisch konsequent wäre eine Gliederung aller Sicherheitsmaßnahmen anhand der Schutzfunktionen und Sicherheitsaspekte wie im NIST Cybersecurity Framework und in NIST SP 800-53 (siehe 4.10.2 und 4.10.3). Eine Zuordnung zu Anwendungsbereichen, wie sie derzeit die Bausteine des Grundschutz-Kompendiums vornehmen, könnte dann – wie in ISO/IEC 27002 vorgesehen – über Klassifizierungen mit zugeordneten Attributen geschehen (siehe 4.2.2, „‚Themes‘ und ‚Attributes‘“).
- Sicherheitsanforderungen lassen sich auch so gliedern, dass sie direkt als Vorlage für Richtlinien verwendet werden können, was eine erhebliche Einsparung von Aufwand bedeutet (siehe Australien, 4.16.2).
- Eine Verlinkung von Grundschutz-Anforderungen mit weiteren operativen Umsetzungshinweisen und Handlungsanweisungen, z. B. nach dem Vorbild Australiens, würde großen Mehrwert bringen.
- Die Wirksamkeit von Maßnahmen gegen real beobachtete Cyberattacken, die nationale Cybersicherheits-Behörden viel besser ermitteln können als einzelne private Organisationen, sollte in die Festlegung von Prioritäten einfließen. Belgien und Australien haben hierfür vorbildliche Ansätze.
- Ein Abgleich mit MITRE ATT&CK wäre eine im Detail wichtige und wirkungsvolle Anreicherung des IT-Grundschutzes.

Aufwand für die Umsetzung des IT-Grundschutzes

- Eine als Ziel angegebene Einsparung von Aufwand gegenüber ISO/IEC 27001 ist zweifelhaft, realistisch scheint eher ein ungefähr vergleichbarer Aufwand (siehe 4.3.7).
- Eine Variante für einen leichten Einstieg in den Grundschutz, über die Basis-Absicherung hinaus vereinfacht, wäre wünschenswert (siehe 5.6).

Breite Anwendbarkeit

- Eine Anwendbarkeit für kleine Unternehmen ist auch nach Aussage des BSI selbst nicht gegeben (siehe 4.3.7).
- Eine reduzierte Fassung des IT-Grundschutzes mit anschaulicherer, deutlich verkürzter Wiedergabe der Methodik sowie weiteren Abkürzungen gegenüber der Basisabsicherung könnte dabei helfen (siehe 5.6 und z. B. 4.7 über Polen).
- Als vereinfachte Umsetzungshilfe zur ISO/IEC 27001 für kleine und mittlere Unternehmen erscheint die deutsche VdS 10000-Richtlinie (siehe 4.7) vorbildlich.
- Die britischen „Cyber Essentials“ sind ein vorbildliches Paket für den Einstieg in Cybersicherheit und kleinere und mittlere Unternehmen, mit einem kleinen Paket an Anforderungen, dessen Umsetzung aber konsequent forciert wird. (siehe 4.18).
- Die Formulierung der BSI-Standards und des Grundschutz-Kompendiums sollte um behördenspezifische Formulierungen bereinigt werden (siehe 4.3.7).

Umfang und Dokumentation des IT-Grundschutzes

- Es wäre eine klarere, kompaktere, anschaulichere und begrifflich sauberere Präsentation der Standards 200-1 und -2 (siehe 4.3.3, 3.2) möglich.
- Ein Zusammenlegen der Standards 200-1 und 200-2 würde auch diesem Ziel dienen (siehe 4.3.3).
- Andere Ansätze kommen mit deutlich kürzeren Beschreibungen der Vorgehensweisen aus (siehe z. B. 4.6 Estland, 4.6.3 Schweiz, 4.7 Polen).

Dokumentationsaufwand in der Anwendung des IT-Grundschutzes

- Die Hilfestellungen für Richtlinien und andere Vorgabedokumente sind nicht ausreichend, was zu vermeidbarem Aufwand bei der Anwendung des IT-Grundschutzes führt (siehe 4.3.5):
  - Zentrale Vorgaben zur Dokumentenlenkung im Standard 200-2 und Baustein ISMS.1 fehlen.
  - Die Gesamtzahl der bei genauer Befolgung zu erstellenden Dokumente ist zu hoch.
  - Eine mögliche Dokumentenstruktur für Richtlinien fehlt.
  - In Grundschutz-Anforderungen verlangten Dokumente fehlen oft Hinweise zu darin zu behandelnden Themen.
  - Eine inhaltliche Abgrenzung verwandter Dokumente ist aus den Grundschutz-Anforderungen oft nicht ersichtlich.
- Auch der Aufwand für die Dokumentation von Nachweisen ist zu hoch (siehe ebenfalls 4.3.5).
- Das zur laufenden Überarbeitung des IT-Grundschutzes veröffentlichte Material nennt zwar die Reduktion des Dokumentationsaufwandes als Ziel, aber nicht alle zuvor genannten Aspekte.
- Die saudi-arabischen Essential Cybersecurity Controls liefern einen vollständigen Satz direkt verwendbarer Vorlagen für Richtlinien und andere Vorgabedokumente – verknüpft mit der in vielen Ansätzen anzutreffenden Sammlung von „Controls“ (siehe 4.17).

8 Anhang

8.1 Definition von Grundbegriffen

8.1.1 Informationssicherheit und Cybersicherheit

[…]

8.1.2 Definition von Sicherheitsanforderungen und -maßnahmen im IT-Grundschutz-Kompendium

[…]

8.2 Recherchierte Länder für ganzheitliche Ansätze zur Cyber- oder Informationssicherheit

[…]

8.3 Dokumentationsanforderungen in ISO/IEC 27001 und 27002

[…]

8.4 Anmerkungen zur Beschreibung der IT-Grundschutz-Methodik in den BSI-Standards 200-1 und 200-2

8.4.1 Bestandteile eines ISMS und Sicherheitsstrategie

[…]

8.4.2 Die Begriffe „Sicherheitskonzept“ und „Sicherheitskonzeption“

[…]

8.4.3 Die Schritte des Sicherheitsprozesses

[…]

8.5 Vorgehensweisen der IT-Grundschutz-Methodik

[…]

8.6 Erforderliche Vorgabedokumente laut IT-Grundschutz-Kompendium

[…]

8.7 Anforderungen mit fehlenden Umsetzungshinweisen im Grundschutz-Kompendium

[…]

8.8 Kommentierung des Textbeispiels zur Überarbeitung des IT-Grundschutzes

[…]

8.9 Kapitelstruktur und Auszug aus dem Österreichischen Informationssicherheitshandbuch

[…]

8.10 Sicherheitsanforderungen des Schweizer IT-Grundschutz

[…]

8.11 Automatisierte Übersetzung der Webseite zum estnischen Informationssicherheits-Standard E-IST

[…]

8.12 Ausschnitte aus dem Estnischen Standard für ISMS

[…]

8.13 Ausschnitte aus dem estnischen IT-Sicherheitskatalog

[…]

8.14 Best Practices des polnischen PPHS Cybersecurity Standard

[…]

8.15 Template zur Erstellung von CSF Profiles

[…]

8.16 An Unternehmen gerichtete Veröffentlichungen der Allianz für Cybersicherheit

[…]

8.17 Beispielmaßnahme aus den belgischen Cyber Fundamentals

8.18 Beispielhafte Maßnahmen aus dem portugiesischen NCF-PT

[…]

[…]

8.19 Maßnahmen der israelischen Cyber Defense Doctrine für Kategorie A-Unternehmen

[…]

8.20 Maßnahmen der israelischen Cyber Defense Doctrine für Kategorie B-Unternehmen

[…]

8.21 Cyber Security Principles des australischen Information Security Manual

[…]

8.22 Kapitel des australischen Information Security Manual

[…]

8.23 Domains und Subdomains der saudi-arabischen Essential Cybersecurity Controls

[…]

8.24 Beispielhafte Anforderungen der britischen „Cyber Essentials“

[…]

8.25 Die britischen „10 Steps to Cyber Security”

[…]

8.26 Technische Maßnahmen der dänischen Effective Cyber Defence

[…]

8.27 Die kanadischen Top 10 IT security actions

[…]

8.28 Anzahl von Google-Suchergebnissen für ISO/IEC 27001, NIST CSF und IT-Grundschutz

[…]

8.29 MITRE ATT&CK Enterprise Tactics

[…]

8.30 MITRE ATT&CK Enterprise Mitigations

[…]

8.31 Abgleich ausgewählter MITRE ATT&CK Techniques und Mitigations mit dem IT-Grundschutz

[…]

9 Literaturverzeichnis

[1] H. Kersten, J. Reuter und K.-W. Schröder, IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz - Der Weg zur Zertifizierung, 4. Aufl., Wiesbaden: Springer Vieweg, 2013.

[2] H. Kersten, G. Klett, J. Reuter und K.-W. Schröder, IT-Sicherheitsmanagement nach der neuen ISO 27001 - ISMS Risiken Kennziffern Controls, 2. Aufl, Wiesbaden: Springer Vieweg, 2020.

[3] H. Kersten und K.-W. Schröder, ISO 27001:2022/2023, Wiesbaden: Springer Vieweg, 2023.

[4] M. Brenner, N. Gentschen-Felde und W. e. a. Hommel, Praxisbuch ISO/IEC 27001 – Management der Informationssicherheit und Vorbereitung auf die Zertifizierung, 4. Aufl., München: Carl Hanser Verlag, 2022.

[5] T. Liedtke, Informationssicherheit – Möglichkeiten und Grenzen, Berlin: Springer Gabler, 2022.

[6] E. Humphreys, „The Future Landscape of ISMS Standards," *Datenschutz und Datensicherheit,* pp. 421-423, 7 2018.

[7] BSI Bundesamt für Sicherheit in der Informationstechnik, „BSI-Standard 200-1 Managementsysteme für Informationssicherheit (ISMS) Version 1.0," 2017a.

[8] Information Security Forum Ltd., „Standard of Good Practice for Information Security," 2024. [Online]. Available: https://www.securityforum.org/solutions-and-insights/standard-of-good-practice-for-information-security/. [Zugriff am 01 06 2024].

[9] A. Deane und A. Kraus, The Official ISC2 CISSP CBK Reference, 6th Edition, New Jersey: John Wiley & Sons, Inc., 2021.

[10] C. Eckert, IT-Sicherheit, 10. Aufl., Berlin/Boston: De Gruyter, 2018.

[11] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley, 2020.

[12] International Organization for Standardization and International Electrotechnical Commission, „ISO/IEC 27100:2020 Information technology — Cybersecurity — Overview and concepts," Genf, 2020.

[13] Wikipedia, „Cybernetics," 18 06 2024. [Online]. Available: https://en.wikipedia.org/wiki/Cybernetics. [Zugriff am 18 06 2024].

[14] Oxford English Dictionary, „cyberspace,“ [Online]. Available: https://www.oed.com/dictionary/cyberspace_n?tab=meaning_and_use#12786295. [Zugriff am 18 06 2024].

[15] Oxford English Dictionary, „Cybersecurity,“ [Online]. Available: https://www.oed.com/dictionary/cybersecurity_n. [Zugriff am 18 06 2024].

[16] International Organization for Standardization and International Electrotechnical Commission, „ISO/IEC 27032:2023 Cybersecurity — Guidelines for Internet security,“ Genf, 2023.

[17] Y. K. S. e. a. Jean-Baptiste Michel, „Quantitative analysis of culture using millions of digitized books,“ 16 12 2010. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3279742/. [Zugriff am 10 06 2024].

[18] Google, „Google Books Ngram Viewer,“ 2019. [Online]. Available: https://books.google.com/ngrams. [Zugriff am 10 06 2026].

[19] International Organization for Standardization and International Electrotechnical Commission, „ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary,“ Genf, 2018.

[20] National Institute of Standards and Technology (NIST), USA, „NIST SP 800-53 Rev. 5 - Security and Privacy Controls for Information Systems and Organizations,“ 2020.

[21] Bundesamt für Sicherheit in der Informationstechnik BSI, „IT-Grundschutz-Kompendium,“ 2023.

[22] National Institute of Standards and Technology NIST, USA, „The NIST Cybersecurity Framework (CSF) 2.0,“ 2024.

[23] International Organisation for Standardization, „ISO deliverables,“ [Online]. Available: https://www.iso.org/deliverables-all.html. [Zugriff am 01 06 2024].

[24] International Organization for Standardization and International Electrotechnical Commission, „ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements,“ Genf, 2022.

[25] S. J. Henk C. A. van Tilborg, Encyclopedia of Cryptography and Security, 2nd edition, New York: Springer New York, 2011.

[26] International Organization for Standardization and International Electrotechnical Commission, „ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls," Genf, 2022.

[27] K. Haufe, „Maturity based approach for ISMS governance, PhD thesis," Madrid, 2017.

[28] K. Haufe und S. Dzombeta, Management-System zur Informationssicherheit – Aufbau und Betrieb gemäß Prozess-Referenzmodell der ISO/IEC TS 27022, Schäffer-Poeschel, 2024.

[29] BSI Bundesamt für Sicherheit in der Informationstechnik, „BSI-Standard 200-2 Version 1.0," IT-Grundschutz-Methodik, 2017b.

[30] Bundesamt für Sicherheit in der Informationstechnik BSI, „Ein Vierteljahrhundert Informationssicherheit: IT-Grundschutz mit Methode," 08 10 2019. [Online]. Available: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2019/25-Jahre-IT-Grundschutz_07102019.html. [Zugriff am 10 06 2024].

[31] Wikipedia, „IT-Grundschutz," 30 04 2024. [Online]. Available: https://de.wikipedia.org/wiki/IT-Grundschutz. [Zugriff am 10 06 2024].

[32] Bundesamt für Sicherheit in der Informationstechnik BSI, „IT-Grundschutz-Kataloge, 15. Ergänzungslieferung 2016," 2016.

[33] Bundesamt für Sicherheit in der Informationstechnik BSI, „BSI-Standard 100-2 IT-Grundschutz Methodology," 2008.

[34] Bundesministerium des Innern BMI, „Umsetzungsplan Bund 2017," Berlin, 2017.

[35] Bundesamt für Sicherheit in der Informationstechnik BSI, „Weg in die Basis-Absicherung (WiBA)," [Online]. Available: https://www.bsi.bund.de/dok/WIBA. [Zugriff am 01 03 2024].

[36] Bundesamt für Sicherheit in der Informationstechnik BSI, „Aktuelles und Diskussion zum IT-Grundschutz," 2023b.

[37] Bundesamt für Sicherheit in der Informationstechnik BSI, „Arbeitsbeispiel RECPLAST".

[38] Bundesamt für Sicherheit in der Informationstechnik, „Die Lage der IT-Sicherheit in Deutschland," Bonn, 2023.

[39] Bundeskanzleramt Österreich, „Österreichisches Informationssicherheitshandbuch Version 4.4.0," Wien, 2023a.

[40] Bundeskanzleramt Österreich, „Österreichisches Informationssicherheitshandbuch,“ 11 2023b. [Online]. Available: https://www.sicherheitshandbuch.gv.at/. [Zugriff am 21 05 2024].

[41] Bundeskanzleramt Österreich, „Österreichisches Informationssicherheitshandbuch 4.3.3,“ 2023c.

[42] Bundesamt für Cybersicherheit BACS, Schweiz, „Sicherheitsverfahren,“ 01 01 2024. [Online]. Available: https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren.html. [Zugriff am 16 05 2024].

[43] Nationales Zentrum für Cybersicherheit NCSC, Schweiz, „Si001 – IT-Grundschutz in der Bundesverwaltung,“ 2022.

[44] Nationales Zentrum für Cybersicherheit NCSC, Schweiz, „P041 – Schutzbedarfsanalyse,“ 2023.

[45] Information System Authority, Republic of Estonia, „Estonian information security standard (E-ITS),“ 29 04 2024. [Online]. Available: https://www.ria.ee/en/cyber-security/management-state-information-security-measures/information-security-standard-e-its. [Zugriff am 09 05 2024].

[46] Information System Authority, Estland, „Estonian Security System Overview,“ 2019.

[47] Ettevõtlus- ja infotehnoloogiaministri (Estnisches Ministerium für Unternehmen und Informationstechnologie), „Eesti infoturbestandardi põhidokumendid (Schlüsseldokumente des estnischen Informationssicherheitsstandards),“ 2023. [Online]. Available: https://eits.ria.ee/. [Zugriff am 09 05 2024].

[48] Ettevõtlus- ja infotehnoloogiaministri (Estnisches Ministerium für Unternehmen und Informationstechnologie), „Eesti infoturbestandard Nõuded infoturbe halduse süsteemile (Estnischer Informationssicherheitsstandard Anforderungen an Managementsysteme für Informationssicherheit),“ 16 12 2022a. [Online]. Available: https://eits.ria.ee/. [Zugriff am 09 05 2024].

[49] Ettevõtlus- ja infotehnoloogiaministri (Estnisches Ministerium für Unternehmen und Informationstechnologie), „Eesti infoturbestandard Etalonturbe kataloog (Estnischer Standard für Informationssicherheit Maßnahmenkatalog),“ 16 12 2022b. [Online]. Available: https://eits.ria.ee/. [Zugriff am 09 05 2024].

[50] VdS Schadenverhütung GmbH, „VdS 10000 – Informationssicherheits-Managementsstem für kleine und mittlere Unternehmen (KMU),“ Köln, 2018.

[51] VdS Schadenverhütung GmbH, „VdS 10005 – Mindestanforderungen an die Informationssicherheit für Klein- und Kleinstunternehmen," Köln, 2020.

[52] VdS Schadenverhütung GmbH, „Cyber Security / Weitere Lösungen & Produkte," [Online]. Available: https://vds.de/kompetenzen/cyber-security/weitere-loesungen-produkte. [Zugriff am 01 06 2024].

[53] Polish Platform for Homeland Security, „PPHS Cybersecurity Standard," 2019. [Online]. Available: https://standard-cyber.ppbw.pl/en/. [Zugriff am 20 04 2024].

[54] Polish Platform for Homeland Security, Polen, „PPHS Cybersecurity Standard," 2020a.

[55] National Institute of Standards and Technology NIST, „Notional CSF 2.0 Profiles Template," 03 2024. [Online]. Available: https://www.nist.gov/profiles-0. [Zugriff am 01 03 2024].

[56] National Institute of Standards and Technology NIST, „CSF 2.0 Implementation Examples," 02 2024. [Online]. Available: https://www.nist.gov/document/csf-20-implementation-examples-xlsx. [Zugriff am 28 02 2024].

[57] Cyber Risk Institute, USA, „CRI Profile v2.0," 2024.

[58] Cybersecurity and Infrastructure Security Agency, „Commercial Factilities Sector – Cybersecurity Framework Implementation Guidance," 2020.

[59] National Cybersecurity Center of Excellence, USA, „Examples of Community Profiles," 2024. [Online]. Available: https://www.nccoe.nist.gov/examples-community-profiles. [Zugriff am 24 05 2024].

[60] National Institute of Standards and Technology (NIST), USA, „FIPS PUB 199 - Standards for Security Categorization of Federal Information and Information Systems," Gaithersburg, 2004.

[61] National Institute of Standards and Technology (NIST), USA, „NIST SP 800-53B - Control Baselines for Information Systems and Organizations," 2020.

[62] MITRE Engenuity, „Sightings Ecosystem: A data-driven Analysis of ATT&CK in the Wild," 2021.

[63] International Organization for Standardization and International Electrotechnical Commission, „ISO/IEC TR 27103: Cybersecurity and ISO and IEC Standards," Genf, 2018.

[64] International Organization for Standardization and International Electrotechnical Commission, „ISO/IEC TS 27110: Cybersecurity framework development guidelines," 2021.

[65] Bundesamt für Sicherheit in der Informationstechnik, „Organisationsplan des BSI," Bonn, 2023.

[66] Bundesamt für Sicherheit in der Informationstechnik, „Allianz für Cyber-Sicherheit," [Online]. Available: https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/home_node.html. [Zugriff am 10 06 2024].

[67] Bundesamt für Sicherheit in der Informationstechnik BSI, „Unternehmen allgemein," [Online]. Available: https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/unternehmen-allgemein_node.html. [Zugriff am 10 06 2024].

[68] Centre for Cybersecurity Belgium, „CyberFundamentals Framework," ohne Datum. [Online]. Available: https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework. [Zugriff am 24 01 2024].

[69] Centre for Cyber security Belgium, „Cyber Fundamentals Basic Version 2023-03-01," 2023.

[70] Centre for Cyber security Belgium, „Cyber Fundamentals Small, Version 2023-03-01," 2023.

[71] Portuguese National Cybersecurity Centre, „National Cybersecurity Framework," 2020.

[72] National Cyber Directorate, Israel, „Managing the the Risk: Full Applied Guide to Organizational Cyber Defense (Cyber Defense Doctrine 2.0)," 06 2021. [Online]. Available: https://www.gov.il/en/departments/general/cyber_security_methodology_2. [Zugriff am 19 01 2024].

[73] National Cyber Security Authority, Israel, „Cyber Defense Methodology for an Organization Ver 1.0," 2017.

[74] National Institute of Standards and Technology, USA, „Success Story: Israel National Cyber Directorate Version 2.0," 11 04 2022. [Online]. Available: https://www.nist.gov/cyberframework/success-stories/israel-national-cyber-directorate-version-20. [Zugriff am 26 05 2024].

[75] National Cyber Directorate, Israel, „ICDM controls," 2021.

[76] Australian Signals Directorate, „Information Security Manual," 2024b.

[77] Australian Signals Directorate, „Information Security Manual (ISM),“ 01 03 2024a. [Online]. Available: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism. [Zugriff am 01 03 2024].

[78] Australian Signals Directorate, „System Security Plan Annex Template (March 2024),“ 03 2024. [Online]. Available: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism. [Zugriff am 01 03 2024].

[79] Australian Signals Directorate, „Strategies to Mitigate Cyber Security Incidents,“ 2017.

[80] Australian Signals Directorate, „Strategies to Mitigate Cyber Security Incidents – Mitigation Details,“ 2017.

[81] Australian Signals Directorate, „Essential Eight Explained,“ 11 2023. [Online]. Available: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-explained. [Zugriff am 01 03 2024].

[82] Australian Signals Directorate, „Essential Eight Assessment Process Guide,“ 07 11 2023. [Online]. Available: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-assessment-process-guide. [Zugriff am 01 03 2024].

[83] National Cybersecurity Authority Saudi Arabia, „Essential Cybersecurity Controls (ECC),“ 2018. [Online]. Available: https://nca.gov.sa/en/legislation?item=191&slug=controls-list. [Zugriff am 28 02 2024].

[84] National Cybersecurity Authority Saudi Arabia, „Guide to Essential Cybersecurity Controls (ECC) Implementation,“ 2023. [Online]. Available: https://nca.gov.sa/en/legislation?item=669&slug=guidelines-list. [Zugriff am 28 02 2024].

[85] National Cybersecurity Authority Saudi Arabia, „Cybersecurity Toolkits,“ 2024. [Online]. Available: https://nca.gov.sa/en/legislation?item=665&slug=guidelines-list. [Zugriff am 28 02 2024].

[86] National Cyber Security Centre UK, „Cyber Essentials: Requirements for IT infrastructure v3.1,“ 2023.

[87] Cabinet Office, UK, „Procurement Policy Note: Updates to the Cyber Essentials Scheme“.

[88] IASME Consortium, „Get Ready for Cyber Essentials,“ [Online]. Available: https://getreadyforcyberessentials.iasme.co.uk/. [Zugriff am 15 04 2024].

[89] Government Communications Security Bureau, Neuseeland, „ISM Document,“ 02 2024. [Online]. Available: https://www.nzism.gcsb.govt.nz/ism-document. [Zugriff am 15 04 2024].

[90] Cyber Security Agency of Singapore, „SG Cyber Safe Programme for Organisations,“ 18 06 2024. [Online]. Available: https://www.csa.gov.sg/our-programmes/support-for-enterprises/sg-cyber-safe-programme. [Zugriff am 18 06 2024].

[91] National Cyber Security Centre, Neuseeland, „NCSC Cyber Security Framework,“ 28 02 2023. [Online]. Available: https://www.ncsc.govt.nz/resources/ncsc-cyber-security-framework?url=resources%2Fncsc-cyber-security-framework%2F. [Zugriff am 15 04 2024].

[92] Bundesamt für wirtschaftliche Landesversorgung BWL, Schweiz, „IKT-Minimalstandard,“ 14 11 2023. [Online]. Available: https://www.bwl.admin.ch/bwl/de/home/bereiche/ikt/ikt_minimalstandard.html. [Zugriff am 15 04 2024].

[93] Department of the Environment, Climate and Communications. Irland, „Public Sector Cyber Security Baseline Standards,“ 16 11 2022. [Online]. Available: https://www.gov.ie/en/publication/d1fd5-cyber-security-baseline-standards/. [Zugriff am 31 01 2024].

[94] Communications Security Establishment Canada, „IT security risk management: A lifecycle approach (ITSG-33),“ 01 11 2012. [Online]. Available: https://www.cyber.gc.ca/en/guidance/it-security-risk-management-lifecycle-approach-itsg-33. [Zugriff am 17 06 2024].

[95] Canadian Centre for Cyber Security, „Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089),“ 09 2021. [Online]. Available: https://www.cyber.gc.ca/en/guidance/top-10-it-security-actions-protect-internet-connected-networks-and-information-itsm10089. [Zugriff am 21 12 2023].

[96] Centre for Cybersecurity, Denmark, „Effective Cyber Defence,“ 2 10 2023. [Online]. Available: https://www.cfcs.dk/en/forebyggelse/guidance/effective-cyber-defence/. [Zugriff am 09 05 2024].

[97] National Cybersecurity Authority, Ministry of Digital Governance Greece, „Cybersecurity Handbook,“ 06 2021. [Online]. Available: https://mindigital.gr/wp-content/uploads/2022/09/Cybersecurity-Handbook-English-version.pdf. [Zugriff am 31 01 2024].

[98] National Cyber Security Centre Ireland, „12 Steps zu Cyber Security," 10 2018. [Online]. Available: https://www.ncsc.gov.ie/pdfs/Cybersecurity_12_steps.pdf. [Zugriff am 24 01 2024].

[99] National Cyber Security Centre UK, „10 Steps to Cyber Security," 11 05 2021. [Online]. Available: https://www.ncsc.gov.uk/collection/10-steps. [Zugriff am 05 11 2023].

[100] National Cyber Security Centre UK, „Cyber Assessment Framework V3.2," 2024.

[101] National Cyber Security Centre UK, „Cyber Security Toolkit for Boards," 23 10 2023. [Online]. Available: https://www.ncsc.gov.uk/collection/board-toolkit. [Zugriff am 15 04 2024].

[102] Government of Canada, „Get Cyber Safe Guide for Small and Medium Businesses," 21 05 2024. [Online]. Available: https://www.getcybersafe.gc.ca/en/resources/get-cyber-safe-guide-small-and-medium-businesses. [Zugriff am 17 06 2024].

[103] Bundesamt für Sicherheit in der Informationstechnik BSI, „IT-Grundschutz – A systematic basis for information security," 2022. [Online]. Available: https://www.bsi.bund.de/dok/it-grundschutz-en. [Zugriff am 10 06 2024].

[104] International Standards Organization, „The ISO Survey," [Online]. Available: https://www.iso.org/the-iso-survey.html. [Zugriff am 15 03 2024].

[105] Bundesamt für Sicherheit in der Informationstechnik BSI, „ISO 27001-Zertifikate auf der Basis von IT-Grundschutz," [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Listen/Zertifikate-ISO-27001-auf-Basis-von-IT-Grundschutz/zertifikate-iso-27001-auf-basis-von-it-grundschutz_node.html. [Zugriff am 29 01 2024].

[106] Bundesamt für Sicherheit in der Informationstechnik BSI, „Zuordnungstabelle ISO zum IT-Grundschutz," 2023.

[107] National Institute for Standards and Technology (NIST), USA, „800-53-v5-to-ISO 27001-2022 Informative Reference Details," 2023.

[108] MITRE Corporation, „MITRE ATT&CK: Design and Philosophy," 3 2020. [Online]. Available: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf. [Zugriff am 22 03 2024].

[109] Wikipedia, „Mitre Corporation,“ [Online]. Available: https://de.wikipedia.org/wiki/Mitre_Corporation. [Zugriff am 27 05 2024].

[110] MITRE Corporation, „Enterprise tactics,“ [Online]. Available: https://attack.mitre.org/tactics/enterprise/. [Zugriff am 27 05 2024].

[111] MITRE Corporation, „Enterprise Techniques,“ [Online]. Available: https://attack.mitre.org/techniques/enterprise/. [Zugriff am 27 05 2024].

[112] MITRE Corporation, „Enterprise Matrix,“ [Online]. Available: https://attack.mitre.org/matrices/enterprise/#. [Zugriff am 29 05 2024].

[113] MITRE Corporation, „Working With ATT&CK,“ 01 04 2024. [Online]. Available: https://attack.mitre.org/resources/working-with-attack/. [Zugriff am 16 04 2024].

[114] MITRE Corporation, „ATT&CK Data & Tools,“ [Online]. Available: https://attack.mitre.org/resources/attack-data-and-tools/. [Zugriff am 29 05 2024].

[115] MITRE Corporation, „Toward a Knowledge Graph of Cybersecurity Countermeasures,“ 2021.

[116] MITRE Corporation, „DEFEND - A knowledge graph of cybersecurity countermeasures,“ [Online]. Available: https://d3fend.mitre.org/. [Zugriff am 29 05 2024].

[117] MITRE Corporation, „Frequently Asked Questions,“ [Online]. Available: https://d3fend.mitre.org/faq/. [Zugriff am 30 05 2024].

[118] Bundesamt für Sicherheit in der Informationstechnik BSI, „XML-Version des IT-Grundschutz-Kompendiums (Edition 2023),“ 2023.

[119] Polish Platform for Homeland Security, Polen, „Best Practices for Management Staff,“ 2020b.

[120] PPHS Polish Platform for Homeland Security, Polen, „Best Practices for IT-Administrators,“ 2020c.

[121] PPHS Polish Platform for Homeland Security, Polen, „Best Practices for Employees,“ 2020d.

[122] Centre for Cyber security Belgium, „Cyber Fundamentals Important Version 2023-03-01,“ 2023.

[123] Centre for Cyber security Belgium, „Cyber Fundamentals Essential Version 2023-03-01,“ 2023.

[124] Wikipedia, „Information security management,“ 23 02 2024. [Online]. Available: https://en.wikipedia.org/wiki/Information_security_management. [Zugriff am 20 04 2024].

[125] R. Moen und C. Norman, „Evolution of the PDCA Cycle,“ 2009.

[126] R. D. Moen und C. L. Norman, „Clearing up myths about the Deming cycle and seeing how it keeps evolving,“ 11 2010. [Online]. Available: https://www.apiweb.org/circling-back.pdf. [Zugriff am 29 01 2024].

[127] J. Hunter, „The Deming Institute,“ [Online]. Available: https://deming.org/the-history-and-evolution-of-the-pdsa-cycle/. [Zugriff am 29 01 2024].

[128] L. Erikson, „How I use the MITRE D3FEND Matrix to defend against ATT&CK(s),“ 18 09 2023. [Online]. Available: https://medium.com/@lerikson/how-i-use-the-mitre-d3fend-matrix-to-defend-against-att-ck-s-9f98cb23df60. [Zugriff am 30 04 2024].

[129] National Institute of Standards and Technology (NIST), USA, „NIST SP 800-53A rev. 5 - Assessing Security and Privacy Controls in Informations Systems and Organizations,“ Gaithersburg, 2022.

[130] National Institute of Standards and Technology, „NIST CSF 2.0: Small Business Quick-Start Guide,“ 2024.

[131] National Institue of Standards and Technology, „NIST CSF 2.0: Quick-Start Guide for Creating and Using Organizational Profiles,“ 2024.

[132] National Cybersecurity Authority, Ministry of Digital Governance Greece, „National Cybersecurity Strategy 2020-2025,“ 12 2020. [Online]. Available: https://mindigital.gr/wp-content/uploads/2022/11/E%CE%9D-NATIONAL-CYBER-SECURITY-STRATEGY-2020_2025.pdf.

[133] NIST National Institute of Standards and Technology, USA, „Framework for Improving Critical Infrastructure Cybersecurity Version 1.1,“ 2018.

[134] Australian Signals Directorate, „Essential Eight Maturity Model FAQ,“ 23 04 2024. [Online]. Available: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model-faq. [Zugriff am 04 05 2024].

[135] Australian Signals Directorate, „Essential Eight Maturity Model and ISM Mapping,“ 01 12 2023. [Online]. Available: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model-ism-mapping. [Zugriff am 01 03 2024].

[136] Australian Signals Directorate, „Essential Eight Maturity Model,“ 27 11 2023. [Online]. Available: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model. [Zugriff am 01 03 2024].

[137] Australian Signals Directorate, „Essential Eight,“ [Online]. Available: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight. [Zugriff am 01 03 2024].

[138] Bundesamt für Sicherheit in der Informationstechnik, „Cyber-Sicherheit für KMU – Die Top 14 Fragen“.

[139] NCSA National Cyber Security Authority, Israel, „Cyber Defense Methodology for an Organization Ver. 1.0,“ 2017.

[140] National Institute of Standards and Technology NIST, „CSF 2.0 Informative References,“ 05 03 2024. [Online]. Available: https://www.nist.gov/informative-references. [Zugriff am 03 05 2024].

[141] Nationales Zentrum für Cybersicherheit NCSC, Schweiz, „P042 - Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept),“ 2023.

[142] MITRE Corporation, „Getting started with ATTACK,“ 10 2019. [Online]. Available: https://www.mitre.org/sites/default/files/2021-11/getting-started-with-attack-october-2019.pdf. [Zugriff am 11 2023].

[143] MITRE Corporation, „MITRE D3FEND - Frequently Asked Questions,“ [Online]. Available: https://d3fend.mitre.org/faq/. [Zugriff am 01 03 2024].

[144] Communications Security Establishment, Kanada, „Baseline cyber security controls for small and medium organizations,“ 02 2020. [Online]. Available: https://www.cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations. [Zugriff am 15 04 2024].

[145] Canadian Centre for Cyber Security, „Top measures to enhance cyber security for small and medium organizations (ITSAP.10.035),“ 02 2024. [Online]. Available: https://www.cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035. [Zugriff am 15 04 2024].

10 Abbildungsverzeichnis

11 Tabellenverzeichnis

12 Verzeichnis der Abkürzungen

ATT&CK	Adversarial Tactics, Techniques and Common Knowledge
BSI	Bundesamt für Sicherheit in der Informationstechnik
CISSP	Certified Information Systems Security Professional
CSF	Cybersecurity Framework
D3FEND	Detection, Denial and Disruption Framework Empowering Network Defense
IEC	International Electrotechnical Commission
ISB	Informationssicherheitsbeauftragter
ISM	Information Security Manual
ISMS	Informationsicherheits-Managementsystem
ISO	International Standards Organization
NIST	National Institute of Standards and Technology
TR	Technical Report
TS	Technical Specification

13 Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Hilfsmittel benutzt habe.

Die Stellen der Arbeit, die anderen Quellen im Wortlaut oder dem Sinn nach entnommen wurden, sind durch Angaben der Herkunft kenntlich gemacht. Dies gilt auch für Zeichnungen, Skizzen, bildliche Darstellungen sowie für Quellen aus dem Internet.

Ich erkläre ferner, dass ich die vorliegende Arbeit in keinem anderen Prüfungsverfahren als Prüfungsarbeit eingereicht habe oder einreichen werde.

Die eingereichte schriftliche Arbeit entspricht der elektronischen Fassung. Ich stimme zu, dass eine elektronische Kopie gefertigt und gespeichert werden darf, um eine Überprüfung mittels Anti-Plagiatssoftware zu ermöglichen.

Berlin, 30.06.2024

Ort, Datum

Unterschrift