HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

BACHELORARBEIT

Herr
Mark Le Corre

Analyse von IT-Notfallmanagement-Standards und -Normen im Kontext von KMU

2020

Fakultät: Angewandte Computer- und Biowissenschaften

BACHELORARBEIT

Analyse von IT-Notfallmanagement-Standards und -Normen im Kontext von KMU

Autor:
Herr Mark Le Corre

Studiengang:
IT-Forensik/Cybercrime

Seminargruppe:
CC16w1-B

Erstprüfer:
Prof. Dr. rer. pol.
Dirk Pawlaszczyk

Zweitprüfer:
M. Sc. Philipp Engler

Einreichung:
Mittweida, 31.07.2020

Faculty of Applied Computer Sciences & Biosciences

BACHELOR THESIS

Analysis of IT emergency management standards and norms in the context of SMEs

author:
Mr. Mark Le Corre

course of studies:
Digital forensics/Cybercrime

seminar group:
CC16w1-B

first examiner:
Mr. Prof. Dr. rer. pol.
Dirk Pawlaszczyk

second examiner:
Mr. M. Sc. Philipp Engler

submission:
Mittweida, 31.07.2020

Bibliografische Angaben

Le Corre, Mark:

Analyse von IT-Notfallmanagement-Standards und -Normen im Kontext von KMU

58 Seiten, Hochschule Mittweida, University of Applied Sciences, Fakultät Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2020

Kurzzusammenfassung

Die Einführung eines IT-Notfallmanagement kann auf freiwilligen Basis oder durch rechtliche Verpflichtungen erfolgen. Hierbei ist die Verwendung von etablierten Standards und Normen gerade für kleine und mittelständische Unternehmen (KMU) empfehlenswert, aber herausfordernd. In der vorliegenden Bachelorarbeit werden einschlägige gesetzliche Verpflichtungen für KMU betrachtet. Es wird sodann auf bekannte Normen und Standards des IT-Notfallmanagements eingegangen. Mit einer selbstentwickelten Methode werden diese auf ihre KMU-Tauglichkeit geprüft. Das Ziel besteht darin, den verpflichteten KMU den für sie geeignetsten der betrachten Standards und Normen aufzuzeigen.

Bibliographic Information

Le Corre, Mark:

Analysis of IT emergency management standards and norms in the context of SMEs

58 Pages, Hochschule Mittweida, University of Applied Sciences, Fakultät Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2020

Abstract

The introduction of an IT emergency management system can be carried out on a voluntary basis or through legal obligations. The use of established standards and norms is recommendable, but challenging, especially for small and medium-sized enterprises (SMEs). In the present bachelor thesis relevant legal obligations for SMEs are considered. It then deals with known norms and standards of IT emergency management. With a self-developed method these are tested for their suitability for SMEs. The goal is to show the obligated SMEs the most suitable of the standards and norms under consideration.

Inhaltsverzeichnis

Abkürzungsverzeichnis

§ ..... Paragraph
Abs. ..... Absatz
AG ..... Aktiengesellschaften
AktG ..... Aktiengesetz
Art. ..... Artikel
ASL ..... Average Sentence Length
ASW ..... Average Number of Syllables per Word
B3S ..... branchenspezifischer Sicherheitsstandard
B3S Gesundheit ..... B3S für die Gesundheitsversorgung im Krankenhaus
BCM ..... Business Continuity Management
BCMS ..... Business Continuity Management System
BSI ..... Bundesamt für Sicherheit in der Informationstechnik
BSIG ..... BSI-Gesetz
bzw. ..... beziehungsweise
ca. ..... zirka
CEN ..... Europäisches Komitee für Normung
CENELEC ..... Europäisches Komitee für Elektrotechnische Normung
COBIT ..... Control Objectives for Information and related Technology
DIN ..... Deutsches Institut für Normung e. V.
DSGVO ..... Datenschutzgrundverordnung
emp. U. ..... empirisch Untersuchung
etc. ..... et cetera
ETSI ..... Europäisches Institut für Telekommunikationsnormen
FRE ..... Flesch-Reading-Ease
gem. ..... gemäß
GmbH ..... Gesellschaft mit beschränkter Haftung
GmbHG ..... Gesetz betreffend die Gesellschaften mit beschränkter Haftung
HGB ..... Handelsgesetzbuch
IEC ..... Internationale Elektrotechnische Kommission
ISMS ..... Managementsysteme für Informationssicherheit
ISO ..... Internationale Normenorganisation
IT ..... Informationstechnik
ITIL ..... IT Infrastructure Library
IT-Sicherheitsgesetz ..... Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme
ITU ..... Internationale Fernmeldeunion
KGaA ..... Kommanditgesellschaften auf Aktien
KMU ..... kleine und mittlere Unternehmen
KRITIS ..... Kritische Infrastruktur
Mio. ..... Million
n. a. ..... nicht auswertbar
Nr. ..... Nummer
OWiG ..... Gesetz über Ordnungswidrigkeiten
PDF ..... Portable Document Format, Portable Document Format
Rn. ..... Randnummer
S. ..... Seite
SME ..... small and medium-sized enterprises

u. a. ..... unter anderem
vgl. ..... vergleiche
WpHG ..... Wertpapierhandelsgesetz
z. B. ..... zum Beispiel
ZDH ..... Zentralverband des Deutschen Handwerks

Formelverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Die Digitalisierung der Unternehmen und Behörden nimmt spürbar zu. In einigen Bereichen sind Unternehmen bereits verpflichtet digital vernetzt zu sein. Beispielsweise müssen sie grundsätzlich seit 2012 Steuererklärungen elektronisch an das Finanzamt übermitteln [2] oder bald im Gesundheitsbereich die elektronische Patientenakte, im Sinne des Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz), einführen [3]. Darüber hinaus sind der Bund, die Länder und die Kommunen gemäß § 1 Absatz 1 Onlinezugangsgesetz verpflichtet bis Ende 2022 ihre Verwaltungsleistungen elektronisch anzubieten. Damit soll unter anderem (u. a.) die Interaktion zwischen Unternehmen und Verwaltung effizienter, nutzerfreundlicher sowie beschleunigt werden [4].

Auch für die Aufrechterhaltung sowie Verbesserung der Wettbewerbsfähigkeit ist die digitale Transformation nahezu unerlässlich. Die Industrie- und Handelskammern führten eine Online-Umfrage im November 2017 durch. Es nahmen 1.806 Unternehmen verschiedener Wirtschaftszweige teil. Zur Frage nach den Auswirkungen von Digitalisierung gaben 44 % der Unternehmen an, dass sie dadurch ihre Umsätze erhöhen konnten und 67 % sehen Chancen durch neue Geschäftsmodelle. Allerdings rechneten dreiviertel (75 %) der Befragten mit einer Steigerung von Sicherheitsrisiken. Mehr als jeder zweite Befragte sieht rechtliche Unsicherheiten (65 %) oder Probleme durch fehlende Standards (60 %). [5, S. 2–23]

Im vergangenen Jahr führte der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom) im zweiten Quartal eine repräsentative Befragung von 1.070 Unternehmen, mit mindestens zehn Mitarbeitern, zum Thema Wirtschaftsschutz durch. Zur Frage, ob das Unternehmen in den letzten zwei Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen war, teilten 75 % ihre Betroffenheit mit und weitere 13 % vermuteten dies. Hierbei gaben kleine Unternehmen, mit 10 bis 99 Mitarbeitern, nahezu die gleiche Betroffenheit an (79 %) wie Unternehmen mit 500 oder mehr Mitarbeitern (78 %). Die Studie beleuchtete ebenfalls die unterschiedlichen Arten der Delikte. Knapp einem Drittel (32 %) wurden IT- oder Telekommunikationsgeräte entwendet und ca. jedem Fünften (21 %) sensible digitale Daten beziehungsweise (bzw.) Informationen. Digitale Angriffe haben bei 70 % der Befragten zu Schäden geführt. Der berechnete Schaden wird mit 102.900.000.000 Euro angegeben. Damit liegt beinahe eine Verdoppelung (55 Milliarden Euro) zur vorangegangenen Befragung im Jahr 2017 vor. Ungefähr jeder zweite Interviewte (48 %) gab an, ein Notfallmanagement in Bezug auf Datendiebstahl, Industriespionage oder Sabotage etabliert zu haben. [6, S. 5–38] In Deutschland gab es im Jahr 2018 3.483.691 Unternehmen mit sozialversicherungspflichtigen Beschäftigten. Davon haben 3.103.896 (ca. 89 %) weniger als zehn Beschäftigte. Der Anteil an Unternehmen mit bis zu 249 Beschäftigten liegt bei ca. 99,56 %

(3.468.239). [7] Insofern nur die Beschäftigtenkennzahl herangezogen wird, würde der Großteil der Unternehmen nach Europäischer Definition zu den kleinen und mittleren Unternehmen (KMU) zählen. Unter Berücksichtigung der vorgenannten Erhebungslage lässt sich auf mehr als 1.500.000 KMU schließen, die kein Notfallmanagementsystem verwenden. Wie aus der Befragung hervorgeht und an späterer Stelle belegt wird, ist das IT-Notfallmanagement ein Bestandteil des Notfallmanagements. Dies liegt nicht zuletzt daran, dass entstehende Notfälle beispielsweise durch Brände, Naturkatstrophen und Stromausfälle auch Auswirkungen auf die verwendete Informationstechnik haben kann [8, S. 1-8].

Bei der Gefährdungslage und fortschreitenden Digitalisierung liegt es nicht fern anzunehmen, dass die Unternehmen verpflichtet sind, sich auf schädigende Ereignisse umfangreich vorzubereiten. Insbesondere, wenn die zu erwartenden Auswirkungen gravierende Folgen haben können oder sogar die Existenz des Unternehmens bedrohen. Dabei überrascht es dennoch eher nicht, wenn von den KMU, denen eher begrenzte personelle und finanzielle Mittel zur Verfügung stehen, weniger als jedes zweite ein Notfallmanagementsystem verwendet [6, S. 38]. Welche Managementsysteme verwendet werden und wer diese installiert hat, geht aus der Befragung nicht hervor.

Die Einführung eines solchen Managementsystems ist ein anspruchsvolles Unterfangen. Es können verschiedene Fehler mit teilweise erheblichen Auswirkungen gemacht werden. So kann beispielsweise ein veralteter Stand der Technik genutzt werden. [9, S. 5] Strebt ein KMU die Einführung eines IT-Notfallmanagements an, sollte es sich daher an anerkannte Standards oder Normen halten. Die Implementierung ist zwar grundsätzlich freiwillig [10], sie bietet jedoch diverse Vorteile. Dazu zählen u. a. Kompatibilität zu anderen Produkten und Dienstleistungen, Rechtssicherheit, Steigerung der Produktsicherheit, die Einbeziehung des Standes der Technik und können zur Effizienzsteigerung führen [11, 7–9].

Diese Bachelorarbeit verfolgt mehrere Ziele. Zunächst werden die wesentlichen gesetzlichen Grundlagen in Hinblick auf die verpflichtende Einführung eines IT-Notfallmanagements zu betrachten. Im Anschluss werden gestellte Norm-Anforderungen sowie deren Prüfbarkeiten bezüglich einer KMU-Tauglichkeit erarbeitet. Diese werden sodann auf in Deutschland gängige IT-Notfallmanagement-Standards und -Normen angewendet. Eine entsprechende Prüfung erfolgt vor dem Hintergrund, den KMU bei der Entscheidungsfindung, welches der verglichenen IT-Notfallmanagement sie unter dem Blickwinkel der Kompatibilität eher einführen können, zu unterstützen. Vorab wird darauf hingewiesen, dass alle angeführten Gesetztestexte in ihrer aktuell geltenden Fassung zitiert wurden. Da sie allgemeine Gültigkeit haben, wird auf die Aufnahme in das Literaturverzeichnis verzichtet. Ausgenommen sind Bezugnahmen auf ältere Fassungen oder zur Hervorhebung.

2 Grundlagen

Für die Betrachtung der späteren Kapitel ist die Erläuterung der nachfolgenden Themen notwendig.

2.1 Unternehmen und Kapitalgesellschaft in Deutschland

Der Begriff Unternehmen ist nicht legal definiert[1]. Gegenwärtig gibt es auch keine Rechtsprechung, die den Unternehmensbegriff im Rahmen des Handelsgesetzbuches, also dem Regelwerk für Kaufleute und den Gewerbetreibenden, explizit darlegt. Innerhalb des HGB wird der Begriff an verschiedenen Stellen verwendet, beispielsweise im Paragraphen (§) 1 Absatz (Abs.) 2 HGB. Dort wird ein Handelsgewerbe wie folgt definiert:

„(2) Handelsgewerbe ist jeder Gewerbebetrieb, es sei denn, daß das Unternehmen nach Art oder Umfang einen in kaufmännischer Weise eingerichteten Geschäftsbetrieb nicht erfordert."

Im § 2 Satz 1 HGB steht:

„Ein gewerbliches Unternehmen, dessen Gewerbebetrieb nicht schon nach § 1 Abs. 2 Handelsgewerbe ist, gilt als Handelsgewerbe im Sinne dieses Gesetzbuchs, wenn die Firma des Unternehmens in das Handelsregister eingetragen ist."

Demzufolge ist nicht jedes Unternehmen ein gewerbliches Unternehmen. Es kommt vielmehr auf den Unternehmensgegenstand an. Der Begriff ist folglich recht weit gefasst. Nach dem bekannten deutschen Wirtschaftswissenschaftler Erich Gutenberg, werden Unternehmen durch die folgenden drei elementaren Merkmale definiert: das erwerbswirtschaftliche Prinzip (Gewinnstreben), Selbstbestimmung des Wirtschaftsplans (Autonomieprinzip) sowie das Alleinbestimmungsprinzip (Unternehmer entscheidet als Eigentümer). [12, 189–192] An einer Legaldefinition des Begriffes Kapitalgesellschaft fehlt es ebenfalls im HGB. Indes zählen, nach dem Titel des zweiten Abschnitts des dritten Buches des HGB, zu den Kapitalgesellschaften die Rechtsformen „Aktiengesellschaften, Kommanditgesellschaften auf Aktien und Gesellschaften mit beschränkter Haftung". Daraus abgeleitet ist eine Kapitalgesellschaft ein gewerbliches Unternehmen, welches einer bestimmten Rechtsform unterfällt.

[1] Legaldefinition bezeichnet die Definition eines Rechtsbegriffes innerhalb eines Gesetzes

2.2 Größenklassen

Unternehmen werden in verschiedene Größenklassen eingeteilt. Je nach Unternehmensgröße resultieren aus der Größenklasse Unterschiede im Zusammenhang mit Förderungen (z. B. im europäischen Rahmenprogramm Horizont 2020[2]), Besteuerungen (u. a. § 19 Umsatzsteuergesetz – Besteuerung der Kleinunternehmer), Betriebsprüfungen (z. B. § 4 Betriebsprüfungsordnung – Umfang der Außenprüfung) oder andere Rechtsfolgen, beispielsweise hinsichtlich der Bilanz (vgl. §§ 266 Abs. 1 Satz 3, 274a HGB) oder Gewinn- und Verlustrechnung (vgl. § 276 HGB).

Die Einteilung der Größenklassen einer Kapitalgesellschaft in klein, mittelgroß und groß ist in Deutschland im § 267 HGB (Umschreibung der Größenklassen) aufgeführt. Ergänzend dazu definiert der § 267a HGB zusätzlich die Kleinstkapitalgesellschaften. Die Einteilungen erfolgen hinsichtlich der Merkmale: Bilanzsumme, Umsatzerlöse und durchschnittlich beschäftigte Arbeitnehmeranzahl. Von diesen Schwellenwerten müssen mindestens zwei der drei, an zwei aufeinanderfolgenden Abschlussstichtagen, über- bzw. unterschritten werden. Für die Einteilung als kleine Kapitalgesellschaften ergeben sich demnach die Merkmale:

- bis 6 Mio. Euro Bilanzsumme,
- bis 12 Mio. Euro Umsatzerlöse in den zwölf Monaten vor dem Abschlussstichtag,
- im Jahresdurchschnitt 50 Arbeitnehmer.

Für die Einordnung als mittelgroße Kapitalgesellschaft ergeben sich die Merkmale:

- bis 20 Mio. Euro Bilanzsumme,
- bis 40 Mio. Euro Umsatzerlöse in den zwölf Monaten vor dem Abschlussstichtag,
- im Jahresdurchschnitt 250 Arbeitnehmer.

Neben den genannten quantitativen Merkmalen gibt es ein qualitatives Kriterium, das ein Unternehmen unabhängig von vorstehenden Schwellenwerten als große Kapitalgesellschaft einstuft. Hierzu muss das Unternehmen eine börsennotierte Aktiengesellschaft gemäß (gem.) § 264d HGB (Kapitalmarktorientierte Kapitalgesellschaft) sein. Börsennotiert sind Gesellschaften, deren Aktien auf einem Markt zugelassen sind, welcher von staatlich anerkannten Stellen geregelt sowie kontrolliert wird und für Publikum mittel- oder unmittelbar zugänglich ist (vgl. § 3 Abs. 1 Aktiengesetz). Das ist gegeben, wenn

[2] Förderungsprogramm für Forschung und Innovation, um unter anderem Europas Wissenschaft zu stärken und Innovationsbarrieren abzubauen sowie dahingehende Zusammenarbeiten zu fördern. [13, S. 40]

Wertpapiere gem. § 2 Abs. 1 Satz 1 Wertpapierhandelsgesetz (WpHG) herausgegeben wurden, die an einem organisierten Markt gem. §2 Abs. 5 WpHG gehandelt werden oder eine Zulassung zum Handel dafür beantragt wurde. Wertpapiere sind in der Begriffsbestimmung im § 2 Abs. 1 WpHG, mit Verweis auf die Verordnung der Europäischen Union 1129/2017, definiert. Demnach sind Wertpapiere unter anderem Aktien, Inhaberschuldverschreibungen, Zertifikate oder Optionsscheine.

Als KMU zählen daher nach dem HGB die Aktiengesellschaft (AG), die Kommanditgesellschaft auf Aktien (KGaA) und Rechtsformen der Gesellschaft mit beschränkter Haftung (GmbH), welche maximal in die Größenklasse der mittelgroßen Kapitalgesellschaft fallen und deren Wertpapiere nur im Freiverkehr gem. § 48 Abs. 1 Börsengesetz gehandelt werden.

Die Abgrenzung der Größenklassen war bis in den Neunzigern des 20. Jahrhunderts europaweit uneinheitlich. Das hatte Auswirkungen auf die Verteilung von staatlichen und europäischen Fördermitteln. Dadurch bestand die Möglichkeit der Wettbewerbsverzerrung, da innerhalb der Mitgliedstaaten unterschiedliche Definitionen von KMU angewendet wurden. Aus diesem Grund wurden in der Empfehlung 92/280/EG der Kommission der Europäischen Gemeinschaften in einem ersten Schritt die Kleinstunternehmen (engl.: micro-sized enterprises) sowie die kleinen und mittleren Unternehmen (engl.: small and medium-sized enterprises (SME)) definiert. Diese trat am 3. April 1996 in Kraft. Mit der Zeit sollten verschiedene Passagen der Empfehlung, insbesondere wegen Interpretationsproblemen, geändert werden. Zur Wahrung der Klarheit hat die Kommission der Europäischen Gemeinschaften am 06. Mai 2003 eine überarbeitete Version verabschiedet, welche die vorangegangene Empfehlung in Gänze ersetzt. Diese findet unter anderem bei der Gewährung von Förderungsmaßnahmen der Europäischen Union Anwendung. Sie gilt seit dem 01. Januar 2005. [14, S. 36]

Unternehmen werden in dieser Empfehlung wie folgt definiert:

„*Als Unternehmen gilt jede Einheit, unabhängig von ihrer Rechtsform, die eine wirtschaftliche Tätigkeit ausübt. Dazugehören insbesondere auch jene Einheiten, die eine handwerkliche Tätigkeit oder andere Tätigkeiten als Einpersonen- oder Familienbetriebe ausüben, sowie Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen.*“ [14, S. 39]

Die Europäische Kommission teilt in ihrer Empfehlung die Unternehmen in Unternehmensklassen ein. Als kleines Unternehmen wird im Wesentlichen definiert, welches

- weniger als 50 Personen innerhalb eines Jahres beschäftigt (in Vollzeiteinheiten, Teilzeitarbeit wird entsprechend umgerechnet) und

- dessen Jahresumsatz oder Jahresbilanz unter 10 Mio. Euro bleibt.

Des Weiteren werden grundsätzlich mittlere Unternehmen als Unternehmen definiert, die

- weniger als 250 Personen beschäftigen (ebenfalls in Vollzeiteinheiten) und
- deren Jahresumsatz 50 Mio. Euro nicht übersteigt oder deren Jahresbilanz maximal 43 Mio. Euro beträgt.

In der Empfehlung sind Einschränkungen genannt, die jedoch keine besonderen Auswirkungen auf den Betrachtungsgegenstand dieser Belegarbeit haben. [14, S. 39]

Es ist zu betonen, dass diese Empfehlung für die Mitgliedsstaaten rechtlich nicht verbindlich ist. Allerdings wird bei EU-Förderungen diese KMU-Definition zu Grunde gelegt. Eine Übersicht der Größenklassen befindet sich auf der Folgeseite (siehe Tabelle 1).

Der Vergleich beider KMU-Definitionen zeigt, dass diese in vielen Teilen voneinander abweichen. Die Definition nimmt mit Ausnahme der geforderten Beschäftigtenzahl teilweise HGB-Merkmale für Kapitalgesellschaften auf, stellt bezüglich der Umsatzerlöse bzw. Bilanzsumme jedoch auf höhere Werte ab. Darüber hinaus inkludieren der Definition auch deutlich mehr Unternehmen, so zum Beispiel die Personengesellschaften. Da die Empfehlung der Europäischen Kommission keine rechtliche Bindung entfaltet, wird für die weitere Betrachtung auf die KMU-Definition nach dem HGB abgestellt.

Unternehmensgröße / Schema nach	Kleinst	Klein	Mittelgroß	Groß
§§ 267, 267a HGB (zwei von drei Merkmalen müssen zutreffen, außer § 264d HGB ist einschlägig, dann Einstufung als große Kapitalgesellschaft)	▪ bis 350.000 Euro Bilanzsumme, ▪ bis 700 000 Euro Umsatzerlöse in den zwölf Monaten vor dem Abschlussstichtag, ▪ im Jahresdurchschnitt 10 Arbeitnehmer	▪ bis 6 Mio. Euro Bilanzsumme, ▪ bis 12 Mio. Euro Umsatzerlöse in den zwölf Monaten vor dem Abschlussstichtag, ▪ im Jahresdurchschnitt 50 Arbeitnehmer.	▪ bis 20 Mio. Euro Bilanzsumme ▪ bis 40. Mio. Euro Umsatzerlöse in den zwölf Monaten vor dem Abschlussstichtag ▪ im Jahresdurchschnitt 250 Arbeitnehmer	▪ über 20 Mio. Euro Bilanzsumme, ▪ über 40 Mio. Euro Umsatzerlöse in den zwölf Monaten vor dem Abschlussstichtag, ▪ im Jahresdurchschnitt mehr als 250 Arbeitnehmer
Empfehlung Kommission Europäischer Gemeinschaft	▪ bis 2 Mio. Euro Jahresbilanz oder Jahresumsatz ▪ weniger als 10 Personen beschäftigt (gerechnet als Vollzeitstellen)	▪ bis 10 Mio. Euro Jahresbilanz oder Jahresumsatz ▪ weniger als 50 Personen beschäftigt (gerechnet als Vollzeitstellen)	▪ bis 50 Mio. Euro Jahresbilanz oder 43 Mio. Euro Jahresumsatz ▪ weniger als 250 Personen beschäftigt (Vollzeiteinheiten)	nicht definiert

Tabelle 1: Übersicht der wesentlichen Einstufungskriterien der Kapitalgesellschaften nach dem Handelsgesetzbuch und der Unternehmen nach der Empfehlung der Kommission Europäischer Gemeinschaft

2.3 Standards

Standards sind für KMU von wichtiger Bedeutung. Durch Vereinheitlichungen können die angebotenen Produkte und Dienstleistungen unternehmensübergreifend angepasst und eine Kompatibilität hergestellt werden. Damit erhöht sich die wirtschaftliche Attraktivität dieser Güter. [11, 3–9] Was als Standard definiert wird, hängt vom betrachteten Kontext ab. Im Bereich der öffentlichen IT ist die nachfolgende Definition gängig:

„*Unter einem Standard verstehen wir eine einheitliche und anerkannte Art und Weise etwas herzustellen oder durchzuführen. Grundlage für einen Standard ist häufig eine technische Spezifikation, deren Inhalt in Form eines Dokumentes festgehalten ist. Eine technische Spezifikation wird dann als Standard bezeichnet, wenn sie in Expertenkreisen hinreichend anerkannt ist und/oder in der Praxis hinreichend akzeptiert und genutzt wird.*“ [15, S. 5]

Generell lassen sich Standards am ehesten als Regelwerk beschreiben, das in Verantwortung einzelner Beteiligter ohne die Öffentlichkeit erarbeitet wurde. Eine Konsesfindung ist nicht erforderlich. Es wird in der Breite des Anwenderkreises akzeptiert und praktisch angewendet. Sie werden zumeist früher als Normen entwickelt. [16, S. 10, 17, S. 56]

Zu den bekannteren Beispielen im IT-Bereich zählen das Betriebssystem Windows, Ethernet, die QWERTY-Tastatur sowie das TCP/IP-Protokoll. [18, 19]

Im Bereich des (IT-)Notfallmanagements gibt es verschiedene nationale und internationale Standardisierungen. [20, S. 5] Vor dem Hintergrund der notwendigen Anerkennung durch die hiesige nationale Behörde für IT-Sicherheit, dem BSI, werden im Folgenden entsprechend geprüfte Sicherheitsstandards betrachtet, welche Regelungen zum IT-Notfallmanagement beinhalten.

Zum einen ist das die Standard-Reihe im Kontext des IT-Grundschutzes des BSI und zum anderen ein branchenspezifischer Sicherheitsstandard (B3S) für die Gesundheitsversorgung im Krankenhaus. Dieser B3S wird ausgewählt, da er auch von kleineren Kliniken angewendet werden kann und aktuell ist. Er ist erst letzten Jahr vom BSI geprüft und akzeptiert worden. [21] Darüber hinaus ist die Systemlandschaft der Krankenhäuser sehr heterogen, wodurch verschiedene IT-Systeme berücksichtigt werden müssen. [22, S. 10]

Zunächst wird auf die Rolle des BSI eingegangen, daran anschließend auf die in Rede stehenden Standards. Hierbei werden im Kurzen u. a. die Inhalte, Prozessbeschreibungen und Bezüge zum IT-Notfallmanagement dargelegt.

2.3.1 Zuständigkeit und Aufgaben des BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist gem. § 1 Satz 2 BSIG „zuständig für die Informationssicherheit auf nationaler Ebene“. Sicherheit in der IT bedeutet demnach „die Einhaltung bestimmter Sicherheitsstandards, welche die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen“ (gem. 2 Abs. 2 BSIG). Zur Informationstechnik (IT) gehören:

„alle technischen Mittel, die der Verarbeitung oder Übertragung von Informationen dienen. Zur Verarbeitung von Informationen gehören Erhebung, Erfassung, Nutzung, Speicherung, Übermittlung, programmgesteuerte Verarbeitung, interne Darstellung und die Ausgabe von Informationen.“ [23]

Die Aufgaben sind geregelt im § 3 BSI-Gesetz (BSIG). Dazu zählen u. a. die Entwicklung von Kriterien und Verfahren für die Prüfung der IT-Sicherheit, Sicherheitszertifikate für IT-Systeme ausstellen sowie das zur Verfügungsstellen von Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen. Hervorzuhebende Ziele des BSI sind die Erstellung und Umsetzung praxisnaher Vorgaben sowie Empfehlungen zur IT-Sicherheit in Zusammenarbeit mit der Wirtschaft [24].

Für die KMU bedeutende Tätigkeiten des BSI sind darüber hinaus die Erstellung von Mindeststandards und Handlungsempfehlungen zur IT-Sicherheit für die Wirtschaft. [24] Das BSI ist damit die nationale Behörde, die sich maßgeblich mit dem Standardisieren des umfassenden Themas IT-Sicherheit beschäftigt.

Da die BSI-Standards ineinandergreifen und eine ganzheitliche Betrachtung angestrebt wird, wird im Folgenden auch auf die Standards eingegangen, die das Thema IT-Notfallmanagement nicht als ausgewiesenen Schwerpunkt haben. Ferner ist hervorzuheben, dass die Standards rund um den IT-Grundschutz das Ziel haben, kompatibel mit internationalen Normen, wie z. B. der ISO 27000-Reihe zur Informationssicherheit oder ISO 31000:2018 zum Risikomanagement, zu sein.

2.3.2 BSI-Standards

Im Folgenden wird zu den relevanten BSI-Standards ausgeführt.

IT-Grundschutz

Das BSI veröffentlicht jährlich den IT-Grundschutz in Form eines IT-Grundschutz-Kompendiums. In dem Kompendium werden im Wesentlichen verschiedene Szenarien betrachtet und Sicherheitsanforderungen anhand der jeweiligen Gefährdungslage beschrieben. Das betrachtete sicherheitsrelevante Thema, wie z. B. Anwendungen, wird IT-Grundschutz-Baustein genannt. Es gibt aktuell zehn derartige Bausteine. Die nachfolgend betrachteten Standards ergänzen das IT-Grundschutz-Kompendium [25].

BSI-Standard 200-1 bis 200-3

Die bekannten Standards zum Thema IT-Grundschutz der Reihen 100-1 bis 100-3 des BSI wurden im Oktober 2017 von den Reihen 200-1 bis 200-3 abgelöst. [19] Die 200er Reihen stellen somit die aktuell gültigen Fassungen dar. Diese enthalten kaum Ausführungen zum Thema Notfallmanagement.

Der Gegenstand des BSI-Standards 200-1 sind Managementsysteme für Informationssicherheit (ISMS). Das BSI definiert:

„*Ein Managementsystem umfasst alle Regelungen, die für die Steuerung und Lenkung der Institution sorgen und somit zur Zielerreichung beitragen. Ein Managementsystem für Informationssicherheit legt somit fest, mit welchen Instrumenten und Methoden die Leitungsebene einer Institution die auf Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenken kann.*“ [26, S. 7]

Der Standard beschreibt den Aufbau eines ISMS mit allgemeinen Anforderungen sowie Empfehlungen für Aufgaben der Leitungsebene. [26, 5–12] Das konkrete Thema (IT-)Notfallmanagement wird in diesem Standard nur nebensächlich beschrieben. Demnach ist die Notfallvorsorge ein Baustein des IT-Grundschutzes, einem 840-seitigen Kompendium bestehend aus 94 Bausteinen. Darüber hinaus wird nur stichpunktartig Bezug in den Bereichen Dokumentation, Notfallübungen, organisatorische Abläufe und Prozesse genommen. [26, S. 18–35]

Im Mittelpunkt des BSI-Standards 200-2 steht eine Methodik zum Aufbau eines ISMS nach IT-Grundschutz. Er baut auf dem BSI-Standard 200-1 auf. Es werden die drei Vorgehensweisen „Basis-Absicherung“, „Kern-Absicherung“ und „Standard-Absicherung“

zur Erstellung einer Sicherheitskonzeption beschrieben (schematischer Aufbau siehe Abbildung 1).

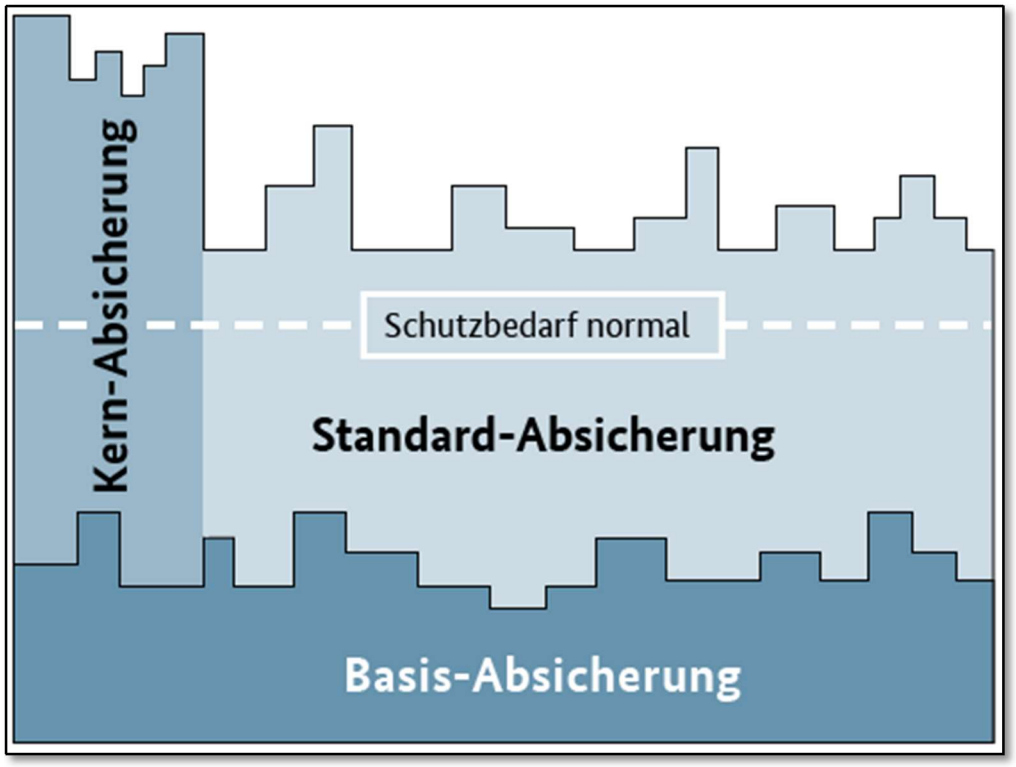


Abbildung 1: drei Varianten der IT-Grundschutz-Absicherung und deren Umfang der Schutzmaßnahmen [27]

Die Basis-Absicherung umfasst eine grundlegende breite Erstabsicherung der relevanten Geschäftsprozesse. Es stellt die niedrigste der drei Absicherungsstufen dar. Die Kern-Absicherung zielt auf eher vereinzelte gefährdete Prozesse ab. Durch diese Maßnahmen, lassen sich die bedeutendsten Ressourcen und Geschäftsprozesse absichern und sind prinzipiell für eine Zertifizierung nach ISO 27001 geeignet. Mit der Standard-Absicherung erfolgt eine umfassende Absicherung in der Breite und Tiefe. Diese Vorgehensweise sollte grundsätzlich zum Schutz der gesamten Institution angestrebt werden und ist die benötigte Grundlage für eine Zertifizierung nach ISO 27001. [28, S. 29–30]

Erwähnt wird das Thema Notfallmanagement im Grunde nur im Kontext von Zuständigkeiten und Aufgaben eines Informationssicherheitsbeauftragten. [28, S. 46]

Der BSI-Standard 200-3 handelt von der Risikoanalyse, welche auf dem IT-Grundschutz des BSI basiert. Risikoanalyse meint in diesem Standard den Prozess, um Risiken beurteilen und behandeln zu können. Zur Beurteilung sind die Identifizierung, Einschätzung

sowie Bewertung von Risiken notwendig. Hier sind einzelne Schritte zur Umsetzung anhand ausgewählter Gefährdungen beschrieben. Das Notfallmanagement findet in diesem Standard keine Berücksichtigung. [29, S. 5–7]

BSI-Standard 100-4

Ein im November 2008 veröffentlichter Standard ist der BSI-Standard 100-4: Notfallmanagement. Dieser hat noch immer Gültigkeit, wird aber voraussichtlich Anfang 2021 vom BSI-Standard 200-4 abgelöst. Zuvor wird der Entwurf der sogenannten „Anwendercommunity“ für Kommentierungen sowie Änderungsvorschläge zur Verfügung gestellt. [30, S. 11–23]

In diesem Standard ist eine Methodik zur Umsetzung und Aufrechterhaltung eines Notfallmanagements geregelt. [20, S. 1] Ein Notfall wird demnach wie folgt definiert:

„*Schadensereignis, bei dem Prozesse oder Ressourcen einer Institution nicht wie vorgesehen funktionieren. Die Verfügbarkeit der entsprechenden Prozesse oder Ressourcen kann innerhalb einer geforderten Zeit nicht wieder hergestellt werden. Der Geschäftsbetrieb ist stark beeinträchtigt. […] Es entstehen hohe bis sehr hohe Schäden, die sich signifikant und in nicht akzeptablem Rahmen auf das Gesamtjahresergebnis eines Unternehmens oder die Aufgabenerfüllung einer Behörde auswirken. Notfälle können nicht mehr im allgemeinen Tagesgeschäft abgewickelt werden, sondern erfordern eine gesonderte Notfallbewältigungsorganisation.*“ [20, S. 5]

Das Notfallmanagement umfasst demzufolge:

„das geplante und organisierte Vorgehen, um die Widerstandsfähigkeit der (zeit-)kritischen Geschäftsprozesse einer Institution nachhaltig zu steigern, auf Schadensereignisse angemessen reagieren und die Geschäftstätigkeiten so schnell wie möglich wieder aufnehmen zu können. Das Notfallmanagement wird auch als „Business Continuity Management“ (BCM) oder „betriebliches Kontinuitätsmanagement“ bezeichnet.“ [20, S. 1]

Das Notfallmanagement beinhaltet die Notfallvorsorge, die Notfallbewältigung wie auch die Notfallnachsorge [20, S. 10]. Ein Bestandteil des Notfallmanagements ist das IT-Notfallmanagement (IT Service Continuity Management) [20, S. 1, 4]. Der Großteil der Geschäftsprozesse einer Institution ist von Informations- und Kommunikationstechnik abhängig [20, S. 105].

Die Phasen eines Notfallmanagements werden in sechs Stufen gegliedert (siehe Abbildung 2).

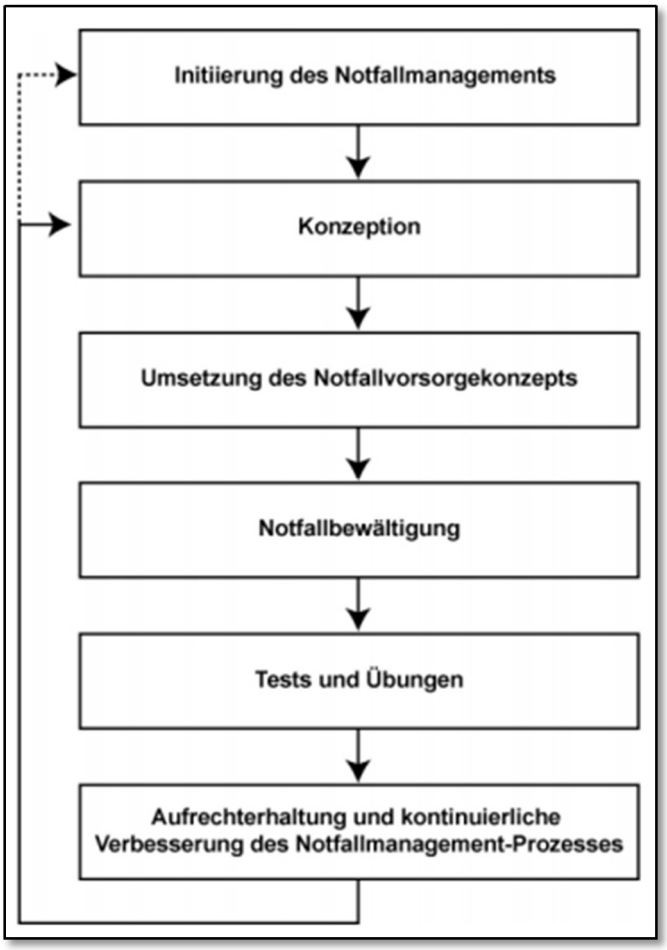


Abbildung 2: Notfallmanagement-Prozess des BSI-Standards 100-4 [20, S. 10]

Bevor ein Notfallmanagement eingerichtet wird, müssen die Randbedingungen geprüft und gegebenenfalls geschaffen werden (Initiierungsphase). Dazu gehören unter anderem die Festlegung der Verantwortlichkeiten, Aufgaben, Schulungen der einbezogenen Personen, Budgetierung und Prüfung der Integration in die Unternehmenskultur. Im nächsten Schritt wird eine Konzeption erstellt. Diese sollten die kritischen Geschäftsprozesse und Ressourcen, deren Priorität zur Wiederherstellung sowie die minimalen Anforderungen an einen möglichen Notbetrieb beschreiben. Des Weiteren sind die jeweiligen Bedrohungen der Geschäftsprozesse sowie Ressourcen auf- und eine Risikoanalyse durchzuführen. Auf Grundlage dieser Erhebungen werden sogenannte Kontinuitätsstrategien entwickelt, die den Rahmen für umzusetzende Vorsorgemaßnahmen bilden. Im nächsten Schritt werden geeignete Notfallvorsorgemaßnahmen konzeptioniert und umgesetzt (Umsetzung des Notfallvorsorgekonzepts). Zu den wichtigsten Vorsorgemaßnahmen gehört die Erstellung eines Notfallhandbuches. Zur Überprüfung und Verbesserung der Notfalldokumente, Prozesse und Abläufe etc. ist die regelmäßige Durchführung von Tests und Übungen bedeutsam. [20, S. 10–11]

Begriffsabgrenzung Risiko- und Notfallmanagement nach BSI

„Nichts geschieht ohne Risiko, aber ohne Risiko geschieht auch nichts“
[Walter Scheel[3]]

Wie im BSI-Standard 100-4 beschrieben, ist das primäre Ziel des Notfallmanagements, präventiv Maßnahmen und Prozesse zu definieren und einzurichten, die dafür sorgen sollen, dass bei Eintritt eines besonders schwerwiegenden Ereignisses zumindest die definierten Minimalanforderungen (z. B. die Verfügbarkeit von bestimmten IT-Services) bereitgestellt werden können. Empfohlen wird die Einrichtung eines solchen Bereiches bei Prozessen mit einem hohen Verfügbarkeitsbedarf. [31, S. 19]

Neben dem Notfallmanagement gibt es noch weitere Managementsysteme, wie das in einigen Gesetzen (siehe Kapitel 3) genannte Risikomanagement. Im Glossar der Cyber-Sicherheit des BSI wird das Risiko definiert als:

„Kombination (also dem Produkt) aus der Häufigkeit, mit der ein Schaden auftritt und dem Ausmaß dieses Schadens. Der Schaden wird häufig als Differenz zwischen einem geplanten und ungeplanten Ergebnis dargestellt. […] Im Unterschied zu "Gefährdung" umfasst der Begriff "Risiko" bereits eine Bewertung, inwieweit ein bestimmtes Schadensszenario im jeweils vorliegenden Fall relevant ist.“ [23]

Unter den Begriff Risikomanagement fasst das BSI die Gesamtheit der Aktivitäten, die im Zusammenhang mit der strategischen und operativen Behandlung von Risiken stehen. [23]

Die beiden genannten Managementsysteme weisen Überschneidungen in ihren Definitionen auf. Eine erkannte Gefährdung (z. B. die Manipulation von gespeicherten Informationen) kann in der individuellen Bewertung als Risiko einer Risikokategorie eingestuft werden [29, S. 27] und anschließend können Maßnahmen zur Risikobehandlung nach dem Risikomanagement ergriffen werden. Bei bedeutsameren Gefährdungen, die etwa das Potential haben, bei Nichtabstellung zu einem unternehmerischen Notfall zu führen, empfiehlt es sich, auf diese nach einem spezielleren System, dem Notfallmanagement, einzugehen. Derartige Beurteilungen und den Schulterschluss der verschiedenen Managementsysteme muss jedes Unternehmen für sich selbst treffen [20, S. 15].

[3] Deutscher Bundespräsident von 1974 bis 1979

2.3.3 B3S Gesundheit

Unternehmen, die zu den sogenannten Kritischen Infrastrukturen zählen, müssen nach § 8a BSIG ein Risiko- und ein Notfallmanagement nachweislich einführen (siehe Kapitel 3.4). Gemäß Absatz 2 können dem BSI branchenspezifische Sicherheitsstandards vorgeschlagen werden. Nach einer Prüfung entscheidet es, ob die gestellten Anforderungen nach Absatz 1 gewährleistet werden. Das BSI hat einen B3S für die Gesundheitsversorgung im Krankenhaus (B3S Gesundheit) am 22.10.2019 akzeptiert [21]. Die Eignungsfeststellung eines B3S wird grundsätzlich für zwei Jahre ausgesprochen. Gegenwärtig wurden B3S in den Sektoren Wasserversorgung sowie Abwasserbeseitigung, Ernährungswirtschaft, Lebensmittelhandel, Informationstechnik, Strom, Fernwärme, Arzneimittel sowie Impfstoffe, Labore, Straßenverkehr und Versicherungen vom BSI angenommen. [32]

Der B3S Gesundheit orientiert sich in seiner Methodik an verschiedenen Quellen (siehe Abbildung 3). Darunter befindet sich die internationale Norm ISO 27001. Diese enthält allgemeingehaltene Anforderungen zur Einrichtung, Umsetzung, Aufrechterhaltung und stetigen Verbesserung eines ISMS sowie für die Beurteilung und Behandlung von Informationssicherheitsrisiken [33, S. 6]. Weitere einfließende internationale Standards sind die IT Infrastructure Library (ITIL) sowie Control Objectives for Information and related Technology (COBIT). ITIL beschreibt Best Practices im Hinblick auf die Einführung, Gestaltung und dem Management von verschiedenen IT-Steuerungsprozessen. [20, 8–9] COBIT stellt ein Rahmenwerk zu Verfügung, welches die strategische Orientierung der IT auf die Geschäftsziele des Unternehmens ausrichtet. Es werden die gesamte Steuerung und Kontrolle der IT-Prozesse sowie der Schutz der IT-Unternehmenswerte erfasst. COBIT unterstützt bei der Verknüpfung von Geschäftsführung und den IT-Steuerungsmodellen (z. B. ITIL). Das Ziel ist die bestmögliche Ausnutzung der IT. Daher werden auch hier Vorteile, Risiken und Ressourcenausnutzung betrachtet. [34, 155–157]

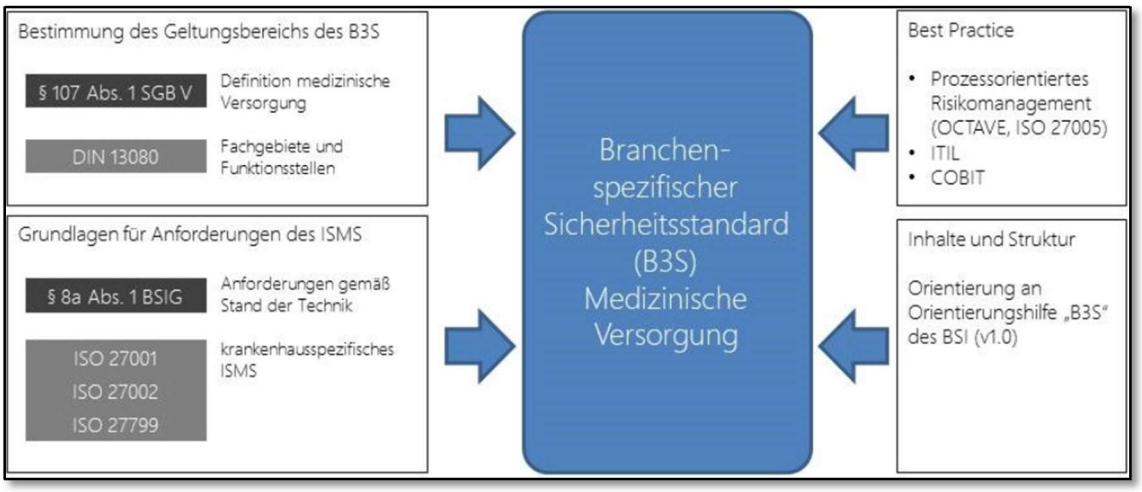


Abbildung 3: Rahmenbedingungen und Quellen zur Erstellung des B3S [22, S. 9]

Der B3S Gesundheit empfiehlt zur Umsetzung der Anforderungen die nachfolgenden Schritte:

Zunächst sollte der Kontext des ISMS festgelegt werden. Dazu zählen u. a. den Geltungsbereich sowie strategische Informationssicherheitsziele festzulegen. Darauffolgend ist die Managementstruktur zu bestimmen und damit in Verbindung stehende Maßnahmen umzusetzen. Im vierten Schritt sind u. a. Risikoobjekte aufzulisten, eine Risikoeinschätzung durchzuführen, Maßnahmen sowie Risikobehandlung für nicht akzeptierte Risiken zu erarbeiten und schriftlich festzuhalten. Anschließend sind die fixierten Maßnahmen umzusetzen. Als Vorletztes wird der entsprechende Schulungsbedarf der Führungskräfte und Mitarbeiter betrachtet. Dieser ist zu ermitteln, ein Durchführungszeitplan zu erstellen und umzusetzen. Der letzte Schritt beinhaltet die Evaluierung des ISMS. [22, S. 12–14]

Auf das Thema Notfallmanagement wird an verschiedenen Stellen eingegangen, z. B. im Kapitel 4 (Risikomanagement in der Informationssicherheit) und Kapitel 7.4 (Betriebliches Kontinuitätsmanagement). Notfallmanagement-Bestandteile finden sich in diversen Anforderungspunkten wie ANF-MN 26 (Notfallpläne sind vom Prozess-/Anwendungsverantwortlichen zu erstellen und aktuell zu halten), ANF-MN 39 (Notfallpläne müssen allen Beteiligten zur Verfügung stehen, ggf. auch Externen) sowie ANF-MN 77 (Maßnahmen in Krisen- und Notfallmanagementplänen müssen vor Einführung priorisiert werden). [22, S. 16–70]

2.4 Normen

Die Einführung und Umsetzung von Normen kommt eine besondere Bedeutung für ökonomische Kompatibilität und Interoperabilität zu. Sie sollen unter anderem zur Wettbewerbsförderung beitragen. [35, S. 12] Eine empirische Studie aus dem Jahr 2011 kommt zu dem Ergebnis, dass Normung das deutsche Wirtschaftswachstum signifikant beeinflusst. Demnach lag der monetäre Anteil am deutschen Wirtschaftswachstum im Zeitraum 2002–2006 bei 16,77 Milliarden Euro pro Jahr. Es sind aber nicht nur geldwerte Vorteile, die die Einführung von Normen bringen. Sie können beispielsweise auch zur Erhöhung der Arbeitsplatzsicherheit oder des Umweltschutzes beitragen. [36, S. 13–19]

Der Begriff der Normung wird nach der DIN EN 45020 definiert als:

„*Tätigkeit zur Erstellung von Festlegungen für die allgemeine und wiederkehrende Anwendung, die auf aktuelle und absehbare Probleme Bezug haben und die Erzielung eines optimalen Ordnungsgrades in einem gegebenen Zusammenhang anstreben.*“ [37, S. 17]

Das Resultat der Normungsarbeit sind Normen. [17, S. 30]

In der europäischen Verordnung Nr. 1025/2012 zur europäischen Normung, wird eine Norm definiert als:

„eine von einer anerkannten Normungsorganisation angenommene technische Spezifikation zur wiederholten oder ständigen Anwendung, deren Einhaltung nicht zwingen ist und die unter eine der nachstehenden Kategorien fällt:

a) ‚internationale Norm‘: eine Norm, die von einer internationalen Normungsorganisation angenommen wurde;

b) ‚europäische Norm‘: eine Norm, die von einer europäischen Normungsorganisation angenommen wurde;

c) ‚harmonisierte Norm‘: eine europäische Norm, die auf der Grundlage eines Auftrags der Kommission zur Durchführung von Harmonisierungsrechtsvorschriften der Union angenommen wurde;

d) ‚nationale Norm‘: eine Norm, die von einer nationalen Normungsorganisation angenommen wurde;“. [35, S. 19]

Die DIN EN 45020 definiert Normen, geringfügig abweichend zur europäischen Verordnung, als ein „Dokument, das mit Konsens erstellt und von einer anerkannten Institution

angenommen wurde und das für die allgemeine und wiederkehrende Anwendung Regeln, Leitlinien oder Merkmale für Tätigkeiten oder deren Ergebnisse festlegt, wobei ein optimaler Ordnungsgrad in einem gegebenen Zusammenhang angestrebt wird“. [37, S. 25] Im Gegensatz zum Wortlaut der europäischen Verordnung, umfassen Normen heutzutage nicht mehr nur technische Regelungen, sondern finden u. a. auch auf Dienstleistungen und Sozialstandards Anwendung. [17, S. 77]

Da eine Norm konsensbasiert, unter Beteiligung aller interessierten Kreise, erarbeitet wird und sich in der Regel auf Anwendungen oder Produkte bezieht, die eine gewisse Marktreife erlangt haben, vergeht bis zur Einführung eine gewisse Zeit. Im Gegensatz zu einer Norm können Standards ohne Einbeziehung aller interessierten Kreise, der Öffentlichkeit, einem vollen Konsens oder Einhaltung von besonderen Fristen zustande kommen. Standards sind häufig die Vorstufe zur Norm. [17, S. 56] Die Normen stellen also eine Untermenge der Standards dar. [16, S. 11]

Die KMU werden als besonders zu berücksichtigender Kreis in der Normungsverordnung der Europäischen Kommission hervorgehoben. Sie sollen insbesondere mit in den Normierungsprozess mit einbezogen und deren nationale Beteiligung erhöht werden. Erreicht werden soll dies unter anderem durch niedrige Normkosten, der Dokumentenübersetzung in die nationale Sprache und einen einfachen Zugang zu den Normen, den Normungsprozessen sowie Informationen zu Normungsvorhaben. [35, S. 12–21]

Zu den europäischen Normungsorganisationen zählen das Europäische Komitee für Normung (CEN), das Europäisches Komitee für Elektrotechnische Normung (CENELEC) sowie das Europäisches Institut für Telekommunikationsnormen (ETSI). [35, S. 28] Zu den von der Europäischen Union anerkannten internationalen Normungsorganisationen gehören gemäß Artikel 2 Nr. 9 die „Internationale Normenorganisation (ISO), die Internationale Elektrotechnische Kommission (IEC) und die Internationale Fernmeldeunion (ITU)“. [35, S. 20]

Die Bezeichnungen von Normen beginnen hierzulande mit den Abkürzungen DIN (deutschen Normen), EN (europäische Norm) oder ISO (internationale Norm). Es können auch mehrere Abkürzungen gleichzeitig auftreten, also beispielsweise DIN EN ISO. In diesem Fall ist die deutsche Ausgabe einer europäischen Norm gemeint, welche mit einer internationalen Norm übereinstimmt. [11, S. 10–11]

Die bedeutendste deutsche Normungsorganisation ist das Deutsche Institut für Normung e. V. (DIN). Sie wird im Rahmen der Deutschen Normungsstrategie von der Bundesregierung als zentrale Normungsorganisation unterstützt und arbeitet in europäischen und internationalen Normungsorganisationen mit. Dort vertritt sie die deutschen Interessen. [38]

Die Anwendung der Normen ist freiwillig, außer es gibt öffentlich-rechtliche oder privatrechtliche verbindliche Bestimmungen. [17, S. 77]

Im Englischen wird sprachlich nicht zwischen Standard und Norm unterschieden. In beiden Fällen heißt es „Standard“. Zur Differenzierung werden allerdings die Zusätze „de jure“ oder „de facto“ verwendet. Der „de jure standard“ ist mit dem deutschen Begriff der Norm und „de facto standard“ nahezu mit dem Begriff Standard gleichzusetzen. [15, S. 6]

Das Deutsche Normenwerk bildet gegenwärtig ca. 34.000 Normen [10]. Im Weiteren werden verbreitete Normen in Deutschland zum IT-Notfallmanagement betrachtet.

2.4.1 DIN EN ISO/IEC 27001

Der bereits angesprochene internationale Standard ISO 27001 ist grundsätzlich Voraussetzung für ein zertifiziertes ISMS. [39] Er gliedert sich in die umfangreiche Normreihe ISO 27000 ein. [40, S. 3] Diese Reihe beinhaltet Normen zur Informationssicherheit und ISMS. [41, S. 6] Die Norm ISO 27001 beschreibt Anforderungen an ein ISMS in Bezug auf die Einrichtung, Umsetzung, Aufrechterhaltung und stetigen Verbesserung eines ISMS sowie für die Beurteilung und Behandlung von Informationssicherheitsrisiken. Sie verweist für verwendete Begriffe wiederum auf die ISO 27000. Demnach wird ein ISMS wie folgt definiert:

„*Ein Informationssicherheitsmanagementsystem (ISMS) umfasst Politik, Verfahren, Richtlinien und damit verbundene Ressourcen und Tätigkeiten, die alle von einer Organisation gesteuert werden, um ihre Informationswerte zu schützen. Ein ISMS ist ein systematisches Modell für die Einführung, die Umsetzung, den Betrieb, die Überwachung, die Überprüfung, die Pflege und die Verbesserung der Informationssicherheit einer Organisation, um Geschäftsziele zu erreichen. Es basiert auf einer Risikobeurteilung und dem Risikoakzeptanzniveau der Organisation und dient dazu, die Risiken wirksam zu behandeln und zu handhaben.*“ [41, S. 21]

Die Definition ist der oben vorgestellten BSI-Definition sehr ähnlich. Ferner werden das Risiko beschrieben als „Auswirkung von Ungewissheit auf Ziele“ [41, S. 16] und das Ziel als „zu erreichendes Ergebnis“ [41, S. 14]. Des Weiteren wird der Begriff Risikoniveau eingeführt als Risikohöhe, die eine Kombination aus Folgen und der Eintrittswahrscheinlichkeit darstellt. [41, S. 13] Erklärungen zum Notfall oder Notfallmanagement sind allerdings weder in der ISO 27000 noch in der ISO 27001 enthalten. Es ist lediglich in der ISO-Norm 27001 zur Anforderung der Aufrechterhaltung der IT-Sicherheit beschrieben, dass dies im Business Continuity Managementsystem geregelt ist. [33, S. 29]

Die ISO 27001 behandelt in ihrem Aufbau verschiedene Bereiche im Zusammenhang mit dem ISMS. Es wird auf den Kontext der Organisation (z. B. Erfordernisse, Erwartungen und Geltungsbereich), die Geschäftsführung, die Planung (zu Risiken sowie Chancen und Informationssicherheitszielen), die benötigten Ressourcen (für die dauerhafte Umsetzung und Verbesserung), den Betrieb mit regelmäßiger Evaluierung, Wirksamkeitsbewertung und Verbesserung eingegangen. Daran anknüpfend werden im Anhang A Referenzmaßnahmen und -ziele tabellarisch beschrieben. Diese 114 Sicherheitsanforderungen sind zu erfüllen, soweit die jeweilige Maßnahme im unternehmerischen Umfeld relevant ist. [40, S. 13] Ist dies nicht der Fall, muss es begründet werden [33, S. 17]. Hinweise zur praktischen Umsetzung der ISO sind nicht vorhanden [20, S. 7].

2.4.2 DIN EN ISO 22301

Mitte des Jahres 2012 wurde erstmals die ISO 22301 veröffentlicht. Es ist die erste internationale und zertifizierbare Norm zum Business Continuity Management (BCM). [42, S. 1] BCM ist ein ganzheitlicher Management-Prozess, der mögliche Bedrohungen einer Organisation und deren wahrscheinliche Auswirkungen auf Geschäftsabläufe identifiziert. Es sollen Kapazitäten aufgebaut werden (Resilienz), um eine effektive Reaktion auf die Bedrohung zu ermöglichen und die Interessen der Organisation sowie der Geschäftspartner zu schützen. [43, S. 8] Ein BCM System (BCMS) wird nach DIN EN ISO 22300 definiert als:

„*Teil des Gesamt-Managementsystems (3.137) zur Einführung und Umsetzung, zum Betrieb sowie zur Überwachung, Überprüfung (3.197), Verwaltung und Verbesserung der Aufrechterhaltung der Betriebsfähigkeit (3.24)“*. [43, S. 8]

Die Aufrechterhaltung der Betriebsfähigkeit wird angegeben als:

„*Fähigkeit einer Organisation (3.21), die Belieferung mit Produkten und Dienstleistungen (3.27) innerhalb akzeptabler Zeiträume mit zuvor festgelegter Kapazität während einer Störung (3.10) fortzusetzen*“. [44, S. 11]

Das Ziel der ISO 22301 ist, Anforderungen an ein BCMS zu stellen, um es dauerhaft zu installieren und zu verbessern. Dadurch schützt es vor Störungen, senkt deren Eintrittswahrscheinlichkeit, verhilft zu Reaktionsmöglichkeiten und gewährleistet jederzeit eine Erholung davon. [43, S. 10]

Der Begriff Risiko wird hier analog zur ISO 27001 definiert. Der Begriff Notfall wird in der Definition eines Zwischenfalls aufgegriffen. Ein Zwischenfall ist „Ereignis, das eine Störung (3.10), ein Verlust, ein Notfall oder eine Krise sein kann oder dazu führen könnte“ [44, S. 13]. Auch wenn weitere Beschreibungen zu dem Begriff fehlen, wird deutlich,

dass eine Gefährdung der Betriebsfähigkeit weitreichende Konsequenzen haben kann, welche mitunter Notfälle auslösen.

Die ISO betrachtet zunächst den Kontext der Organisation (Kapitel 4). Es sind u. a. die (rechtlichen) Anforderungen sowie der Anwendungsbereich zu deklarieren und das BCMS unter den Anforderungen tatsächlich einzuführen. Zu den Aufgaben der Organisationsleitung gehört die Sicherstellung der notwendigen Bedingungen zur Umsetzung der gestellten Anforderungen, inklusive der Überwachung. Sie muss eine Organisationspolitik festlegen und betreiben, welche die Betriebsfähigkeit aufrechterhält. Die mit dem Betrieb zusammenhängenden Rollen, Aufgaben und Befugnisse müssen verteilt und organisationsintern publiziert werden. Das Kapitel 6 handelt von der Maßnahmenplanung zum Umgang von Risiken sowie Chancen. Des Weiteren werden Anforderungen an Ziele und Schritte zur Zielerreichung bezüglich der Betriebsfähigkeitserhaltung festgelegt. Zuletzt werden auch Anforderungen zu etwaige BCMS-Änderungen bestimmt. [44, S. 17–21] Die Planungsphase ist eine kritische Phase, da gesetzten strategischen Ziele und Richtlinien das BCMS gänzlich betreffen. [42, S. 101]

Der darauffolgende Abschnitt greift das Thema Unterstützung auf. Hier werden Anforderungen an benötigte Ressourcen, organisationsbezogene Kompetenzen, Kenntnisse des eingesetzten Personals sowie Kommunikations- und Dokumentationsregelungen formuliert. Nachdem die vorangegangenen Kapitel sich eher mit der Vorbereitung und Planung eines BCMS beschäftigten, handelt Abschnitt 8 von dem (Wirk-)Betrieb. Inhalte sind beispielsweise die Steuerung und Umsetzung der im Kapitel 6 thematisierten Maßnahmen, Anforderungen an eine durchzuführende Business-Impact-Analyse und Risikobeurteilung, Strategieerarbeitung und -umsetzung aus den resultierenden Ergebnissen, eine Reaktionsstruktur etablieren, Kommunikationsstrukturen und ein Warnmeldewesen regeln sowie Pläne zur Aufrechterhaltung der Betriebsfähigkeit erstellen und fortschreiben. Ferner werden Anforderungen an Übungen und Überprüfungen gestellt. Der Abschnitt schließt mit Regelungen zu Bewertungen der wesentlichen in diesem Kapitel aufgeführten Aspekte. [44, S. 21–29]

Das Kapitel 9 beinhaltet ebenfalls das Thema Bewertung. Blickrichtung ist die Leistungsbewertung der von der Organisation selbst festgelegten Bereiche sowie des verwendeten BCMS. Dazu gehören z. B. die regelmäßige Anforderungsprüfung nach der in Rede stehenden ISO, aber auch die Bewertung des BCMS durch die Organisationsleitung. [44, S. 30–32]

Das letzte Kapitel trägt den Titel „Verbesserung“. Damit sollen die beabsichtigte Ergebniserreichung des BCMS gefördert und das BCMS kontinuierlich verbessert werden. [44, S. 32–33]

3 Gesetzliche Verpflichtungen zur Einführung eines IT-Notfallmanagements

Gegenwärtig existiert kein eigenständiges Gesetz mit dem Schwerpunkt IT-Notfallmanagement. Allerdings wurde am 24. Juli 2015 das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) im Bundesgesetzblatt veröffentlicht. [45, S. 1324] Entgegen des Titels ist das IT-Sicherheitsgesetz ein Artikelgesetz, welches andere Gesetze ändert oder ergänzt. Entsprechende Vorschriften finden sich also in verschiedenen Gesetzen mit unterschiedlichen Adressaten und sind damit nur schwer überschaubar. Im Folgenden wird auf die wesentlichen Rechtsnormen eingegangen, die konkrete gesetzliche Verpflichtungen zum Gegenstand haben oder aus denen sich diese ableiten können.

3.1 HGB

Wie im Kapitel 2.1 beschrieben, enthält das Handelsgesetzbuch diverse Regelungen für Kaufleute bzw. Gewerbetreibenden. Zu den Rechtsformen von Kapitalgesellschaften gehören die Aktiengesellschaften, die Kommanditgesellschaften auf Aktien und die Gesellschaften mit beschränkter Haftung.

Kapitalgesellschaften müssen einmal im Jahr einen Jahresabschluss (vgl. § 242 Abs. 1 HGB) erstellen. Zusätzlich muss ein Lagebericht erstellt und veröffentlichen werden (vgl. § 264 Abs. 1 HGB). Von dieser Verpflichtung sind kleine Kapitalgesellschaften und Kleinstkapitalgesellschaften ausgenommen (vgl. § 264 Abs. 1 HGB). Der Lagebericht soll gem. § 289 Abs. 1 HGB die aktuelle Situation des Unternehmens realitätsgetreu widerspiegeln. Er hat unter anderem eine Beurteilung der voraussichtlichen Entwicklung, mit den wesentlichen Chancen und Risiken zu enthalten. Die Risiken müssen begründet werden. Was der Risiko-Begriff nach HGB umfasst, wird darin nicht geklärt.

Mit der Verabschiedung des Artikelgesetzes „Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)“ [46, S. 786] im Jahr 1998 wurden ergänzende Regelungen hinsichtlich des Risikomanagements von Unternehmen implementiert. Unter anderem wurden die aufgezeigten Inhalte des Lageberichtes gem. § 289 Abs. 1 HGB um den folgenden Teilsatz erweitert: „dabei ist auch auf die Risiken der künftigen Entwicklung einzugehen“ [46, S. 789]. Das BSI sieht in diesem Bezug ebenfalls die Erforderlichkeit, dass Unternehmen ausreichende Maßnahmen zur Vorbeugung gegen Krisen und Notfällen treffen [47].

Das Gesetz soll insbesondere die Einrichtung eines Kontrollsystems mit verpflichtenden Regeln im Unternehmen sowie darüber hinaus ein unternehmensweites Risikomanagement etablieren. Damit sollen kritische Entwicklungen für den Fortbestand des Unternehmens erkannt und entgegengewirkt werden. [48, S. 8]

In dem Lagebericht sind zusätzlich auf „die Risikomanagementziele und -methoden der Gesellschaft“ einzugehen (vgl. § 289 Abs. 2 Nr. 1 a HGB). Die Vertreter der Gesellschaft müssen versichern, dass sie nach bestem Wissen den Geschäftsverlauf, inklusive des Geschäftsergebnisses sowie die Lage so dargestellt haben, dass ein den tatsächlichen Verhältnissen entsprechendes Bild vermittelt wird (vgl. § 264 Abs. 2 Satz 3 HGB).

Der Lagebericht dient potentiellen Geschäftspartnern, Kunden und Behörden dazu, einen aussagekräftigen Eindruck über die Entwicklung des Unternehmens zu erhalten. Ferner unterstützt der Bericht auch bei wichtigen Investitionsentscheidungen.

Gemäß § 316 Abs. 1 HGB besteht eine Verpflichtung zur Prüfung des Lageberichtes durch einen Abschlussprüfer. Findet die Prüfung nicht statt, kann der Jahresabschluss der Kapitalgesellschaft nicht festgestellt werden. Der Regelungsgegenstand des § 317 Abs. 2 HGB legt zudem explizit fest, dass die bei der Prüfung des Jahresabschlusses gewonnen Erkenntnisse im Einklang mit dem Lagebericht stehen müssen und er ein zutreffendes Bild des Unternehmens vermittelt. Des Weiteren umfasst die Prüfung demnach die Schlüssigkeit der prognostizierten Chancen und Risiken.

Nach der Prüfung hat der Abschlussprüfer über Art und Umfang sowie dem Ergebnis dieser zu berichten (vgl. § 321 Abs. 1 Satz 1 HGB). Bei der Durchführung der Prüfung muss der Prüfer unter anderem über festgestellte Unrichtigkeiten, Verstöße gegen gesetzliche Vorschriften sowie Tatsachen, welche den Bestand gefährden oder die Entwicklung des geprüften Unternehmens besonders beeinträchtigen, berichten (vgl. § 321 Abs. 1 Satz 3 HGB). Er muss unabhängig sein (vgl. § 321 Abs. 4a HGB) und kann Einwendungen erheben sowie seine Erklärung der Abschlussprüfung entsprechend einschränken (vgl. § 322 Abs. 4 HGB). Dies kann auch vor dem Hintergrund geschehen, „wenn der Abschlussprüfer nach Ausschöpfung aller angemessenen Möglichkeiten zur Klärung des Sachverhalts nicht in der Lage ist, ein Prüfungsurteil abzugeben“ (§ 322 Abs. 5 HGB).

Die entsprechenden Strafvorschriften z. B. wegen unrichtiger Darstellung hinsichtlich des Lageberichts finden sich in § 331 ff. HGB. Auf das Eingehen von weiteren Pflichten und möglichen Ahndungen, beispielsweise bei Verstößen gegen die Offenlegungspflichten des Jahresabschlusses, wird im Rahmen dieser Belegarbeit nicht weiter eingegangen.

3.2 AktG

Das Aktiengesetz (AktG) beinhaltet Regelungen zu Aktiengesellschaften sowie Kommanditgesellschaften auf Aktien. Die Regelungen nach dem HGB bleiben davon unberührt. Wie im Kapitel 2.1 durch das HGB definiert, unterfallen den KMU auch Unternehmen, welche mit Wertpapieren frei handeln. Bei Unternehmungen, die börsennotierte mit Wertpapiere handeln, werden die quantitativen Schwellenwerte ausgehebelt. Sie werden als große Unternehmung behandelt. Viele Regelungen nach dem AktG gelten für börsennotierte und nichtbörsennotierte Gesellschaften gleichermaßen.

Der Vorstand einer Kapitalgesellschaft leitet das Unternehmen unter eigener Verantwortung (gem. § 76 Abs. 1 AktG). Er hat nach § 90 AktG eine Berichtspflicht gegenüber dem Aufsichtsrat. Auch gem. § 170 Abs. 1 AktG ist er verpflichtet, unverzüglich den Jahresabschluss und den Lagebericht dem Aufsichtsrat vorzulegen. Der Aufsichtsrat muss diese gem. § 171 AktG prüfen. Handelt es sich bei der Gesellschaft um eine mittelgroße oder große, muss ein Abschlussprüfer hinzugezogen werden (vgl. § 316 Abs. 1 HGB). Der Abschlussprüfer hat:

„*an den Verhandlungen des Aufsichtsrats oder des Prüfungsausschusses über diese Vorlagen teilzunehmen und über die wesentlichen Ergebnisse seiner Prüfung, insbesondere wesentliche Schwächen des internen Kontroll- und des Risikomanagementsystems bezogen auf den Rechnungslegungsprozess, zu berichten. Er informiert über Umstände, die seine Befangenheit besorgen lassen und über Leistungen, die er zusätzlich zu den Abschlussprüfungsleistungen erbracht hat“* (§ 171 Abs. 1 Satz 2, 3 AktG). Zusätzlich hat der Vorstand nach § 91 Abs. 2 AktG:

„*geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.*“

Eine verpflichtende Prüfung sowie Beurteilung dieser Maßnahmen und des Überwachungssystems gem. § 317 Abs. 4 HGB durch den Abschlussprüfer entfällt allerdings bei KMU, da diese per Definition keine börsennotierten Aktiengesellschaften sein können. Jedoch stellt eine Nichteinführung eines entsprechenden Früherkennungssystems ein Verstoß dar, den der Abschlussprüfer gem. § 321 Abs. 1 Satz 3 HGB in seinem Bericht aufzunehmen hat. Wegen der Bedeutsamkeit dieser Maßnahme gehen Prüfer in der Praxis immer mehr auf die Früherkennung ein. Sie weiten folglich die Regelungen des § 317 Abs. 4 HGB auch auf nicht-börsennotierte Kapitalgesellschaften aus. Bei einer Pflichtverletzung haftet der Vorstand nach § 93 Abs. 2 S. 1 AktG mit seinem privaten Vermögen. [49]

Der Aufsichtsrat muss überdies überprüfen, ob der Vorstand seinen Pflichten nachkommt. Er haftet ebenfalls bei pflichtwidrigem Unterlassen (vgl. §§ 116, 93 AktG). Das Gesetz konkretisiert nicht die genauere Ausgestaltung des Früherkennungssystems oder des Risikomanagements. Des Weiteren ist im § 93 Abs. 1 Satz 1 AktG generalklauselartig normiert, dass die „Vorstandsmitglieder bei der Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden haben“. Diese allgemein gehaltene Regelung muss also bei entsprechenden Tätigkeiten berücksichtigt werden.

3.3 GmbHG

Das Gesetz betreffend die Gesellschaften mit beschränkter Haftung (GmbHG) regelt im Wesentlichen den Sachbereich der GmbH und deren Sonderform. Das Besondere an dieser Handelsgesellschaft ist die grundsätzliche Haftung für Verbindlichkeiten mit dem Gesellschaftsvermögen und nicht mit dem privaten Vermögen (vgl. § 13 GmbHG).

Auch im GmbHG finden sich Regelungen zum Jahresabschluss und Lagebericht. Eine Aufgabe des Geschäftsführers ist die Feststellung des Jahresabschlusses (vgl. § 46 Nr. 1 GmbHG). Nach Aufstellung haben sie diesen sowie den Lagebericht unverzüglich zur Feststellung den Gesellschaftern vorzulegen. Wenn eine Prüfung des Jahresabschlusses durch einen Abschlussprüfer vorzunehmen ist, ist der Prüfbericht mit dem Jahresabschluss sowie den Lagebericht schnellstmöglich den Gesellschaftern bzw. dem Aufsichtsrat vorzulegen (vgl. § 42a Abs. 1 GmbHG). Die Gesellschafter müssen den Jahresabschluss und die Ergebnisverwendung verbindlich beschließen (vgl. § 42a Abs. 2 GmbHG).

Geschäftsführer sind verpflichtet „in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden“ (§ 43 Abs. 1 GmbHG). Insofern die Sorgfalt verletzt wurde und dadurch ein Schaden entsteht, haftet der Geschäftsführer persönlich (vgl. § 43 Abs. 2 GmbHG). Sie sind somit an vorschriftsmäßigen Handeln gebunden und müssen folglich unter anderem Vorteile für die Kapitalgesellschaft wahrnehmen und Schäden von ihr abwenden. Hierbei haben sie einen gewissen Ermessensspielraum. Die Entscheidungen müssen zum Wohle der Kapitalgesellschaft ausgerichtet werden und laut Rechtsprechungen, unter Ausschöpfung sämtlicher verfügbarer Informationsquellen. Darüber hinaus muss der Geschäftsführer eine Übersicht über die wirtschaftliche sowie finanzielle Lage der Gesellschaft haben und falls notwendig, ein Überwachungssystem zur Erkennung und Kontrolle von Risiken installieren. Insofern ein

erhöhtes Risikopotential besteht, kann die Einführung eines Compliance-Management-Systems[4] verpflichtend sein. [50, 51]

3.4 KRITIS-Betreiber nach BSIG in Verbindung mit BSI-KritisV

KMU können zu den Kritischen Infrastrukturen (KRITIS) zählen. Kritische Infrastrukturen werden im § 2 Abs. 10 BSIG definiert als:

„Einrichtungen, Anlagen oder Teile davon, die

1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und

2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden."

In der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) werden die betreffenden Sektoren mit den jeweiligen Schwellenwerten weiter definiert. Aufgrund ihrer besonderen Bedeutung für die Gesellschaft unterliegen KRITIS-Betreiber diversen gesetzlichen Bestimmungen. Sie haben u. a. gemäß § 8a Abs. 1 BSIG:

„angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden."

Die Erfüllung der genannten Anforderungen sind alle zwei Jahre nachzuweisen (vgl. § 8a Abs. 3 BSIG). Da die in Absatz 1 genannten Anforderungen recht allgemein sind, hat das BSI Konkretisierungen veröffentlicht. Demnach müssen die Betreiber ein Risiko- sowie Notfallmanagement implementieren [52, S. 10–13].

---

[4] Compliance-Management, auch als Anforderungsmanagement bezeichnet, inkludiert alle in einer Institution eingerichteten Maßnahmen, die Strukturen, Prozesse und Regelkonformität sicherstellen. [8, S. 109–113]

3.5 Anbieter digitaler Dienste (nach BSIG)

Das BSIG nimmt neben KRITIS Bezug auf Anbieter digitaler Dienste. Das sind gem. § 2 Abs. 12 BSIG juristische Personen, die einen digitalen Dienst anbieten. Weiter konkretisiert Absatz 11, welche Anbieter in die Zielgruppe fallen. Dazu gehören Anbieter von Online-Märkten, Online-Suchmaschinen oder Cloud-Computing-Diensten. Von den Regelungen ausgenommen sind Unternehmen, die nur ihre eigenen Waren in einem Online-Shop anbieten. Der Normzweck zielt viel mehr auf Dienstleister ab, die für Dritte eine Art Infrastruktur bereitstellen. Bei einem Ausfall können negative wirtschaftliche Auswirkungen auf den Großteil der Nutzer entstehen. [53]

Diese genannten Anbieter haben nach § 8c Abs. 1 BSIG technische und organisatorische Maßnahmen zu treffen, um Sicherheitsrisiken der Netz- und IT-Systeme, für die Bereitstellung der digitalen Dienste, zu bewältigen. Gemäß Absatz 2 müssen Maßnahmen auf dem Stand der Technik ergriffen werden, die im angemessenen Verhältnis zu dem Sicherheitsrisiko der Netz- und Informationssysteme stehen. In diesem Kontext ist u. a. der Aspekt des Betriebskontinuitätsmanagements (IT-Notfallmanagement) zu berücksichtigen.

3.6 OWiG

Das Ordnungswidrigkeitengesetz (OWiG) regelt Ahndungen von Rechtsverstößen, die keine Straftaten darstellen. Eine verpflichtende Einführung entsprechender Managementsysteme könnte in diesem Gesetz geregelt sein.

Nach § 130 OWiG handeln Geschäftsführer für Verstöße gegen unterlassene erforderliche Aufsichtsmaßnahmen ordnungswidrig. Das Erfordernis, zur Einführung derartiger Systeme, wie z. B. Compliance-Management-Systeme, lässt sich daraus jedoch nicht für KMU direkt ableiten. Dessen ungeachtet muss der Geschäftsführer Maßnahmen in Abwägung der Art, Größe und Gefahr für Rechtsverletzungen etc. treffen. [54]

3.7 DSGVO

Umfangreichere Regelungen, zu unternehmerischen Verpflichtungen ein Managementsystem zu implementieren, finden sich in der Datenschutzgrundverordnung (DSGVO).

Die DSGVO ist seit dem 25.05.2018 in Deutschland anwendbar. Sie regelt Datenschutzvorschriften zum Umgang mit personenbezogenen Daten, die für alle europäischen Mitgliedstaaten unmittelbar gelten. Darin sind auch sogenannte Öffnungsklauseln enthalten. Die einzelnen Mitgliedstaaten können diese weiter konkretisieren. In Deutschland wird dies durch das zeitgleich wirksam gewordene neue Bundesdatenschutzgesetz (BDSG-neu) umgesetzt. Hinsichtlich der DSGVO muss festgestellt werden, dass der Begriff Risiko häufig verwendet, jedoch nicht definiert wird.

Allerdings wird in dem Erwägungsgrund Nr. 75 DSGVO beschrieben, dass Risiken für die Rechte und Freiheiten natürlicher Personen aus der Verarbeitung von personenbezogenen Daten entstehen können. Risiken sind nach Eintrittswahrscheinlichkeiten sowie Schwere klassifiziert und können zu einem physischen, materiellen oder immateriellen Schaden führen. Ferner sollte nach dem Erwägungsgrund Nr. 76 das jeweilige Risiko anhand von einer objektiven Bewertung beurteilt werden. [55, S. 15]

Der Risikobegriff nach DSGVO zeigt elementare Übereinstimmungen mit dem des BSI. Grundsätze für die Verarbeitung personenbezogener Daten sind im Artikel (Art.) 5 DSGVO geregelt. Auf den Sicherheitsaspekt wird im Art. 5 Abs. 1 Buchstabe f DSGVO wie folgt eingegangen:

„Personenbezogene Daten müssen […] in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit")". [55, S. 35–36]

Ferner wird in Absatz 2 geregelt:

„Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht")". [55, S. 36]

Zu den allgemeinen Pflichten gehört gemäß Art. 24 Abs. 1 DSGVO:

„Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete

technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert." [55, S. 47]

Die Verantwortlichen für die Datenverarbeitung haben gem. Art. 32 Abs. Buchstaben b, c, d DSGVO dauerhaft die CIA-Schutzziele[5] der IT-Sicherheit zu gewährleisten, diese im physischen oder technischen Zwischenfall schnell wiederherzustellen und die Wirksamkeit der getroffenen Maßnahmen zu überprüfen, bewerten und evaluieren. [55, S. 51, 52]

Wird bei einer entsprechenden Datenverarbeitungsform ein hohes Risiko prognostiziert, muss gem. Art. 35 Abs. 1 DSGVO eine Abschätzung der Folgen durchgeführt werden (Datenschutz-Folgeabschätzung). Mindestanforderungen der Abschätzung sind im Absatz 7 geregelt. Demnach müssen u. a. die geplanten Verarbeitungsvorgänge systematisch beschrieben, Risiken bewertet sowie Maßnahmen zur Behandlung der Risiken nachweislich geplant werden.

3.8 Zusammenfassung

Die verpflichtende Einführung eines Notfallmanagements bei den KMU ist im Wesentlichen abhängig von der Größe und dem Geschäftsgegenstand des Unternehmens. Nach dem HGB sind alle Unternehmen verpflichtet, begründend auf aktuelle und zukünftige Risiken im Lagebericht einzugehen. Von der Verpflichtung zur Lageberichtserstellung sind kleine Unternehmen ausgenommen. Obligatorisch ist für Unternehmen, die Wertpapiere frei (nicht börsennotiert) handeln, ein Frühwarnsystem zur Erkennung von gefährdenden Entwicklungen zu betreiben. Dem GmbHG unterfallende Unternehmen haben, bei entsprechendem Risikopotential, ebenso ein Erkennungs- und Kontrollsystem für Risiken einzuführen und Entscheidungen zum Wohle des Unternehmens zu treffen. Ferner sind Anbieter digitaler Dienste nach dem BSIG verpflichtet, ein IT-Notfallmanagement einzuführen. Insbesondere aber die DSGVO setzt hohe Anforderungen an die Datenverarbeitung von personenbezogenen Daten, die von den KMU berücksichtigt werden müssen. Hier sind neben der nachweislichen Prüfung von Risiken ebenfalls entsprechende Gegenmaßnahmen, auch zur Aufrechterhaltung der CIA-Schutzziele der IT-Sicherheit, einzuleiten. Eine Nachweisverpflichtung zur Einführung eines Notfallmanagements obliegt Betreibern kritischer Infrastrukturen.

[5] Confidentiality (Vertraulichkeit), Integrity (Integrität), Availability (Verfügbarkeit)

4 Analyse der Standards und Normen hinsichtlich ihrer KMU-Tauglichkeit

In diesem Kapitel werden Kriterien für eine KMU-Tauglichkeitsprüfung aufgestellt. Als Entscheidungsgrundlage für die einzelnen KMU werden anschließend die vorgestellten Standards und Normen hinsichtlich ihrer KMU-Tauglichkeit analysiert.

4.1 Kompatibilitätskriterien

„Think small first and think practical!“ [56, S. 9]

In den vorherigen Kapiteln wurde aufgezeigt, dass eine Einführung eines mehr oder minder umfangreichen Notfallmanagements für nahezu jedes Unternehmen relevant ist. Für einige ist die Implementierung sogar verpflichtend. Gerade bei einem solch sensiblen und komplexen Thema wie das IT-Notfallmanagement sollten bewährte Anforderungen und Vorgehensmodelle angewendet [42, S. 33]. Die KMU stehen vor der Herausforderung, dies mit eher geringen personellen sowie finanziellen Ressourcen umzusetzen. Normen und Standards dienen den Anwendern als Orientierung zur Implementierung sowie Überprüfung der IT-Systeme und -Infrastruktur im Hinblick auf das Notfallmanagement. Wie in den nachfolgenden Kapiteln beschrieben, bestehen diese aus festgelegten und in gewissen Abständen überprüften Anforderungen.

In der Vergangenheit war die geringe Beteiligung der KMU im Normungs- oder Standardisierungsprozess problematisch. Dadurch wurden die Interessen und Handlungsmöglichkeiten der KMU innerhalb der Europäischen Union nicht ausreichend berücksichtigt. [57, S. 4] Als ein Lösungsansatz wurde im Jahr 2010 ein Leitfaden für die Erstellung von Normen veröffentlicht. Damit sollen die KMU-Bedürfnisse in den Normungsprozess verstärkt integriert werden. Die Beachtung der enthaltenen Hinweise und Empfehlungen ist allerdings freiwillig.

Ausgewählte Aspekte des Leitfadens werden im nachfolgend verkürzt dargestellt:

- Normverständlichkeit der Norm-Adressaten,
- Prüfung und Einbeziehung spezieller KMU-Bedürfnisse,
- Verhältnismäßigkeit der entstehenden Kosten durch Normeinführung,
- Normen müssen den am Markt verfügbaren Stand der Technik widerspiegeln,
- Anforderungen als Leistungsmerkmale ausdrücken,
- Vermittlung von Grundlagenwissen,
- Nutzung von Beispielen, Erklärungen oder Veranschaulichungen,
- Einleitung mit Erstellungsmotivation, Normenziel sowie Zielgruppe,

- konkreten Anwendungsbereich (betroffene Produkte und Dienstleistungen) definieren,
- einfache und eindeutige Überprüfbarkeit der Anforderungsübereinstimmung,
- Normen sollten so kurz wie möglich sein und Querverweise vermeiden,
- gute Übersichtlichkeit und relevante Informationen schnell auffindbar,
- allgemeinverständliche Sprache verwenden,
- Erklärungen von Abkürzungen,
- komplizierte Ausdrücke erklären und ggf. in einem eigenen Kapitel „Begriffe“ aufnehmen,
- Verweisungen auf andere Normen nur wenn nötig, ggf. Text zitieren,
- Norm-Änderungen müssen deutlich sichtbar sein. [57]

Am Ende des Leitfadens befindet sich die in der Abbildung 4 dargestellte Checkliste, über die wesentlichen zu berücksichtigenden Punkte bei der Normenerstellung. Diese sind nach dem chronologischen Verlauf gegliedert.

Vorbereitung des neuen Projektes	**Vorbereitung der Norm**	**Erarbeitung des Inhalts**	**Aufbau und Gestaltung des Inhalts**	**Abschließende Prüfung**
❑ (5.2.1) Wurde die Relevanz der Norm für KMU geprüft? ❑ (5.2.1) Wurde geprüft, ob innerhalb der interessierten Kreise spezielle Bedürfnisse unter den KMU bestehen? ❑ (5.2.2) Wurde untersucht, ob KMU zur Zielgruppe gehören?	❑ (5.3.1) Wurden die Investitionskosten (Technologie, Ausstattung, Prüfungen) ermittelt und bewertet? ❑ (5.3.1) Wurden die Schulungskosten (Personal) bewertet? ❑ (5.3.1) Wurden die Kosten für die Anwendung bewertet? ❑ (5.3.2) Wurde geprüft, ob alle Elemente verfügbar sind	❑ (5.4.1) Wenn der anwendungsbezogene Ansatz angewendet wird, ist er verständlich? ❑ (5.4.2) Wurden anschauliche Erklärungen verwendet? ❑ (5.4.3) Ist der Anwendungsbereich der Norm genau und vollständig? ❑ (5.4.4) Wurden strenge Prüfsysteme vermieden? ❑ (5.4.4) Wurden die Kosten für Prüfungen bewertet? ❑ (5.4.5) Wurden einfache und kosteneffiziente Möglichkeiten, um die Übereinstimmung mit den Anforderungen zu prüfen, ermittelt?	❑ (5.5.1) Ist die Norm so kurz wie möglich? ❑ (5.5.1) Wenn die Norm lang ist, wurde die Möglichkeit in Betracht gezogen, die Norm in kürze Normen aufzuteilen? ❑ (5.5.2) Ist der Aufbau der Norm leicht nachzuvollziehen? ❑ (5.5.3) Wurden unterstützende Schaubilder, Tabellen usw. (wenn möglich) eingefügt? ❑ (5.5.4) Wurde eine klare Sprache verwendet, die von allen erwarteten Normenanwendern verstanden wird? ❑ (5.5.5) Wurde die Anzahl an Referenznormen minimal gehalten? ❑ Wurden klare Informationen über die Änderungen gegenüber Vorgängerversionen der Norm gegeben? (5.5.6)	❑ (5.6.1) Wurde eine Übergangsfrist vorgeschlagen, die die Folgen der Änderungen widerspiegelt? ❑ (5.6.2) Wurde der Bedarf an einem Einführungshandbuch bewertet?

Abbildung 4: Leitfaden-Checkliste [57, S. 13]

Darüber hinaus wurde im Jahr 2012 von dem Europäischen Parlament sowie dem Rat der Europäischen Union eine Verordnung zur Zusammenarbeit der Normungsorganisationen und der Erarbeitung europäischer Normen sowie Dokumente verabschiedet. Darin sind die KMU und deren Normungsmitwirkung besonders verankert, da diese den Großteil der europäischen Unternehmen ausmachen. Die Normungsorganisatoren werden gehalten, die Teilnahme der KMU an der Normungstätigkeit zu fördern und vereinfachen. Ebenfalls soll dieser Zielgruppe der Zugang zu Normen erleichtert werden. [35, S. 14–21]

Gegenwärtig sieht der Zentralverband des Deutschen Handwerks (ZDH) Umsetzungsprobleme von Normen für die ca. eine Million nationale Handwerksbetriebe, welche die Hauptumsetzer der Normen sind. Der ZDH veröffentlichte im Mai 2020 ein Positionspapier, in dem verschiedene Schwierigkeiten formuliert sind, die für die Betriebe, mit durchschnittlich fünf Mitarbeitern, kaum umsetzbar seien. Zu diesen gehören unter anderem

- die Zusammenstellung der für den Betrieb relevanten Normen,
- die aktive Mitarbeit in der Normung, wegen fehlenden zeitlichen, finanziellen und personellen Ressourcen,
- die Normentransparenz,
- die verständliche Formulierung der Normen,
- die Normen-Zugänglichkeit,
- die Übersichtlichkeit des sehr hohen Normenbestandes (allein in Deutschland sind ca. 34.000 Normen im Bestand und jährlich erscheinen rund 2.000 neue DIN-Normen),
- die zunehmenden Querschnittsnormen, ohne konkreten Produktbezug,
- die inhaltlichen und thematischen Norm-Dopplungen,
- die Verständlichkeit und Lesbarkeit, wegen steigender Komplexität und Normenumfang,
- das Normen teilweise nicht umsetzbar sind, da unzureichender am Markt verfügbarer Stand der Technik,
- die Prüfung der „KMU-Tauglichkeit“, also der praktischen Norm-Anwendbarkeit, ist während der Normenerstellung wegen geringer KMU-Beteiligung umsetzbar,
- die Referenzmethoden abschaffen und vereinfachte Rechenverfahren einführen,
- die Sprachbarrieren,
- die Einführung eines KMU-Kompatibilitätstests,
- weitere eher im politischen Bereich angeordnete Probleme. [56, S. 2–9]

Die vielfältigen angebrachten Aspekte aus dem Leitfaden sowie dem Positionspapier des ZDH kristallisieren das Erfordernis, Normen prinzipiell auf KMU-Umsetzungstauglichkeit (Kompatibilität) zu prüfen. Ansonsten kann es zu einer nicht oder nicht richtigen Einführung bzw. Umsetzung von Normen in den KMU führen. Aufgrund der vorgenannten Bandbreite der Punkte sollten in einem solchen Test verschiedene Kriterien geprüft werden, die Einfluss auf die KMU-Umsetzung von Normen haben.

Der Großteil der aufgelisteten Aspekte können zu prüfbaren Kompatibilitätskriterien klassifiziert werden. Diese Kriterien lassen sich in normbezogene Vollständigkeit, Aufbau, Lesbarkeit und Verständlichkeit, Wirtschaftlichkeit und Prüfbarkeit der Anforderungen einteilen. Die Zuordnungen von Kompatibilitätskriterium zu den Aspekten sind in der Tabelle 2 enthalten.

Kompatibilitätskriterien	**Aspekt**
Vollständigkeit der Einleitung	▪ Alle zum Themenfeld gehörige Normen, inklusive Querschnittsnormen sind aufgelistet ▪ Die im Anwendungsbereich genannten Inhalte sind vollständig
Aufbau	▪ Erstellungsmotivation ▪ Benennung Normenziel sowie Zielgruppe ▪ gute Übersichtlichkeit ▪ relevante Informationen schnell auffindbar ▪ nachvollziehbare Versionsänderungen

Kompatibilitätskriterien	Aspekt
Lesbarkeit und Verständlichkeit	▪ leichte Lesbarkeit ▪ allgemeinverständliche Sprache ▪ Abkürzungen sind erklärt ▪ komplizierte Ausdrücke sind erklärt und ggf. in einem Kapitel „Begriffe“ aufgenommen ▪ Vermittlung von Grundlagenwissen ▪ Nutzung von Beispielen, weiteren Erklärungen oder Veranschaulichungen ▪ Normenlänge so kurz wie nötig ▪ Vermeidung von Querverweisen innerhalb der Normen ▪ Vermeidung von Verweisungen auf andere Normen, ggf. Text zitieren ▪ deutsche Sprache ▪ Vermeidung inhaltlicher und thematischer Norm-Dopplungen
Wirtschaftlichkeit	▪ Normen-Zugänglichkeit ▪ Verhältnismäßigkeit der entstehenden Kosten durch Normeinführung ▪ Normen spiegeln den am Markt verfügbaren Stand der Technik wider ▪ vereinfachte Rechenverfahren verwenden
Prüfbarkeit der Anforderungen	▪ definierter Anwendungsbereich ▪ Anforderungen als Leistungsmerkmale ausgedrückt

Tabelle 2: Auflistung Kompatibilitätskriterien und deren Aspekte

Das DIN legt ebenfalls Merkmale zur Erstellung anwenderfreundlicher Normen in der DIN 820, Beiblatt 3:2016-10, Anhang A fest. Diese sind in der Anlage 1 aufgeführt.

4.2 Prüfbarkeit der Kompatibilitätskriterien

Vor dem Hintergrund Normen und Standards hinsichtlich ihrer KMU-Tauglichkeit anhand der oben genannten Kompatibilitätskriterien zu prüfen, werden in diesem Unterkapitel die Aspekte auf Prüf- und Messbarkeit untersucht. Um die Lesbarkeit zu verbessern, wird auf die explizite Nennung des Begriffes Standard oder der standardähnlichen Auslegung verzichtet. Bei der späteren standardbezogenen Untersuchung wird die einzelne Auslegung an angebrachten Stellen erweitert. Dies geschieht aufgrund des von den Normen abweichenden Aufbaus. Die in Rede stehenden Schriftsätze geben selbst keine Prüf- oder Messmethoden und auch keine Schwellenwerte zur Bewertung bekannt. Insofern werden eigene Methoden und Werte erarbeitet und soweit möglich angewendet.

4.2.1 Vollständigkeit der Einleitung

Die hier gestellte Anforderung beinhaltet, dass aus der einzelnen Norm alle zur Umsetzung in Bezug stehenden Normen, inkl. Querschnittsnormen, hervorgehen oder diese darin geregelt sind. [56, S. 3] Die DIN 820-2:2020-03 regelt die Gestaltung von Dokumenten bezüglich der Normungsarbeit. Darin enthalten sind Ausführungen zu diesen normativen Verweisungen. Demnach sind alle zitierten Verweisungen, die Anforderungen darstellen, im Abschnitt 2 (im Bereich der Einleitung bzw. des Vorwortes) zu erfassen. [58, S. 96–97] Diese zusammenhängenden Normen und deren Fehlen können vor allem durch die zuständigen Normungsorganisationen erkannt werden.

Darüber hinaus wird gefordert, dass alle im Anwendungsbereich der Norm genannten Inhalte abgebildet sind. [57, S. 9] Die zuvor angesprochene DIN-Norm führt auch zum Anwendungsbereich aus. Demnach sollen das Thema des Dokumentes sowie die behandelten Sachverhalte im Anwendungsbereich festgelegt sein, inklusive der Anwendbarkeitsgrenzen. So sollen ggf. durch den Anwender themenbezogene anzunehmende Inhalte ausgeschlossen werden, welche in der Norm unberücksichtigt bleiben. [58, S. 94] Darüber hinaus wird ausgeführt:

„*Der Anwendungsbereich muss als Abschnitt 1 nummeriert werden. Er darf unterteilt werden, jedoch ist dies im Allgemeinen nicht notwendig, da er kurz und prägnant abgefasst werden soll.*“ [58, S. 95]

Dieser Aspekt ist durch eine Dokumentensichtung prüfbar.

4.2.2 Aufbau

In einer Norm sollen die Beweggründe, das Normenziel, die Zielgruppe sowie Informationen zu Änderungen der Vorversionen erkennbar enthalten sein. Diese Aspekte sind aus der Norm selbst ablesbar.

Darüber hinaus werden eine gute Übersichtlichkeit sowie das Auffinden relevanter Informationen angebracht. Die Übersichtlichkeit eines Textes wird unter anderem im Kontext von hervorgehobenen Festlegungen, Verdeutlichung von praktischen Normbestandteilen und dem anwenderbezogenen Layout des Textes beschrieben. [57, S. 10–11] Aufgrund fehlender Konkretisierungen, bedarf es in diesem Kontext einer empirischen Untersuchung (emp. U.), um hinreichend prüfbare Kriterien zu finden. Das zügige Auffinden relevanter Informationen ist nicht weiter umschrieben. Eine Abschätzung dessen wäre über eine Befragung der Norm-Anwender möglich. Hinweise auf ein hinreichend schnelles Auffinden können ein Stichwort- sowie Inhaltsverzeichnis oder Kurzbeschreibungen und Zielsetzungen der Kapitel geben. Diese Hinweise werden geprüft.

4.2.3 Lesbarkeit und Verständlichkeit

Im Positionspapier sowie in der Empfehlung zur Normung wird die Lesbarkeit angesprochen. [56, S. 3, 57, S. 10–11] Eine Norm sollte demnach leicht zu lesen sein.

Lesbarkeit wird nach der DIN 1450 definiert als „Eigenschaft leserlich angeordneter Zeichenfolgen, die es ermöglicht, die Information zweifelsfrei zu verstehen“. [59, S. 4]

Klassische Formeln in der Lesbarkeitsforschung, zur Ermittlung des Lesbarkeitsgrades eines Textes, berechnen sich aus statistischen Werten des Textes. Dazu gehören häufig die durchschnittliche Anzahl von Wörtern pro Satz sowie die Silbenanzahl. Damit soll die Verständlichkeit eines Textes mit einem Wert ausgedrückt werden. Zu den bekanntesten Lesbarkeitsindizes gehört der sogenannte Flesch-Index (Flesch-Reading-Ease (FRE)), beschrieben im Jahr 1948 durch Rudolf Flesch. [60, S. 75–78] Dieser wird in drei Schritten berechnet. Zuerst wird die durchschnittliche Satzlänge (Average Sentence Length (ASL)) multipliziert mit 1,015. Sie wird aus der Division von Wortanzahl durch Satzanzahl im Text gebildet. Danach wird die durchschnittliche Silbenanzahl pro Wort (Average Number of Syllables per Word (ASW)) erhoben und mit 84,6 multipliziert. Die durchschnittliche Silbenanzahl errechnet sich aus der Silbenanzahl im Text durch die Anzahl der Wörter im Text. Beide Werte werden summiert und von dem Wert 206,835 subtrahiert (siehe Formel 1). Im Ergebnis erhält man einen Wert von 0 bis 100. Je höher der Wert, desto besser sei die Lesbarkeit. Liegt der Wert beispielsweise zwischen 60 und 70, gilt er demnach als geeignet für 13- bis 15-jährige Schüler. [61]

$$FRE = 206{,}835 - (1{,}015 \bullet ASL) - (84{,}6 \bullet ASW)$$

Formel 1: Flesch-Reading-Ease [61]

Die in der Formel 1 verwendeten Werte beziehen sich auf englischsprachige Texte. Die deutschen Texte haben durchschnittlich mehr Silben pro Wort als die englischen, wodurch diese schwieriger erscheinen, als sie tatsächlich sind. [60, S. 76]

In seiner Dissertation mit dem Titel: „Wie verständlich sind unsere Zeitungen?“ aus dem Jahr 1978 entwickelte Toni Amstad eine Formel für deutschsprachige Texte, die auf dem FRE basiert. Wie bei FRE werden die durchschnittliche Satzlänge (ASL) im Text und das Produkt aus durchschnittlicher Silbenanzahl (ASW) multipliziert mit 58,5 summiert und von dem Wert 180 subtrahiert (siehe Formel 2). Die Lesbarkeitsstufen von 0 bis 100 bleiben erhalten. [zitiert nach 60, S. 76]

$$FRE_{deutsch} = 180 - ASL - (58{,}5 \bullet ASW)$$

Formel 2: Flesch-Reading-Ease für deutschsprachige Texte [zitiert nach 60, S. 76]

Auch wenn die Berechnung aus den Kriterien Wort- und Satzlänge Zweifel hinsichtlich der Aussagekraft aufkommen lassen, stehen diese indirekt in Bezug zu einer ganzen Reihe weiterer Größen, wie beispielsweise die Worthäufigkeit. [62, S. 21–31] Die Anzahl der Sätze, Wörter und Silben der Normen werden im Kontext der späteren Lesbarkeitsbestimmung über die Webseite http://textinspektor.de/text_testen.php5 bestimmt. Vor dem Einlesen der Texte werden die Kopfzeilen auf jeder Seite (S.) entfernt. Der einzulesende Text beginnt ab (mit) der Einleitung, falls keines namentlich existiert, ab (mit) dem Vorwort, bis zum Ende des Dokumentes.

Die Verständlichkeit eines Textes hängt jedoch nicht allein von statistischen Häufigkeiten ab. Um keine Leser auszuschließen und auch Interpretationsfehler zu minimieren, sollten die Normen auch in deutscher Sprache verfasst sein. Neben den im Text verwendeten Fachwörtern können das Vorwissen des Lesers sowie die individuelle kognitive Leistungsfähigkeit und auch standarddeutsche Begriffe verständlichkeitserschwerend wirken [63, S. 147]. Gerade im Prozess der Normerstellung sollten diese daher Punkte in Bezug auf die Textrezipienten (Normenanwender) abgeklärt werden. Das kann durch zielgruppenabhängige empirische Untersuchungen, wie z. B. Umfragen, erfolgen.

In der Praxis wird dies z. B. durch die Messung der Lesezeit eines Textes und dem anschließenden Wiedergeben einer kurzen Zusammenfassung des Gelesenen untersucht. [64, S. 320]

Im Gegensatz zur Norm-Verständlichkeit kann der Aspekt des Erklärens von Abkürzungen ohne Einbeziehung der Ziel-Rezipienten geprüft werden. Die in der Norm enthaltenen Abkürzungen sollten in einem Abkürzungsverzeichnis aufgeführt sein. Die Anforderungen komplizierte oder unklare Ausdrücke zu erklären sowie Grundlagenwissen in einem angemessenen Umfang zu vermitteln, sind abhängig von der Norm sowie den Anwendern. An dieser Stelle empfehlen sich empirische Untersuchungen.

Die Nutzung von Beispielen sowie Veranschaulichungen lassen sich durch das Lesen der Norm (Textabgleich) prüfen.

Die Norm sollte so kurz wie nötig sein. Dies kann durch die Vermeidung von Dopplungen und nicht notwendigen Inhalten sowie kurzen Ausdrucksweisen erreicht werden. Eine Prüfung empfiehlt sich eher durch die praktische Norm-Umsetzung. Das Lesen der Norm ist zur Feststellung von Querverweisen, also den Verweisungen auf andere Stellen in der Norm [57, S. 10] und der verwendeten Sprache ausreichend. Thematische und inhaltliche Norm-Dopplungen sollten durch Norm-Experten, beispielsweise von Normungsorganisationen geprüft werden. Ihnen liegt ein besserer Norm-Überblick vor.

4.2.4 Wirtschaftlichkeit

Das Kompatibilitätskriterium Wirtschaftlichkeit umfasst die Aspekte, welche erkennbaren Einfluss auf das Verhältnis von Ertrag und Aufwand bzw. Kosten haben. Grundsätzlich berechnet sich die Wirtschaftlichkeit aus der Division von Leistung (wertmäßiges Produktionsergebnis) durch Kosten (siehe Formel 3). [65, S. 28]

$$\text{Wirtschaftlichkeit} = \frac{Leistung\ (in\ Geldeinheiten)}{Kosten\ (in\ Geldeinheiten)}$$

Formel 3: Berechnung der Wirtschaftlichkeit

Diese sind durch das einzelne Unternehmen in einer gewissen Zeit mit einem entsprechenden Aufwand abschätzbar. Die Ziel-Norm sowie die mit dieser in Verbindung stehenden Normen müssen gut zugänglich sein [56, S. 3]. Den geringsten Mobilitätsaufwand hat der Zugang über die Webseite des Beuth Verlages, welcher die Normen für das Deutsche Institut für Normung vertreibt [66].

Eine Normeinführung muss für die KMU wirtschaftlich sein. Entstehende Norm-Erwerbskosten sind generell bestimmbar, z. B. über die Webseite des Verlages. Dagegen sind zu treffende Investitionen und deren Umfang individuell, wodurch eine Einzelfallbetrachtung notwendig ist. Abhängig sind die entstehenden Kosten unter anderem von der Unternehmensgröße, dem Geschäftsgegenstand, der infrastrukturellen Anbindung sowie der in der Nähe befindlichen Dienstleister. Vom Grundsatz her kann in Bezug auf IT-

Notfälle, die kritische Auswirkung auf die Betriebserhaltung haben, die Einführung eines IT-Notfallmanagement als rentabel angesehen werden. Ein derartiger Vorfall könnte schlimmstenfalls zur Zerschlagung des Unternehmens führen. In der späteren Prüfbarkeit wird lediglich auf die Anschaffungskosten abgestellt, da diese grundsätzlich für alle KMU gleich sind.

Die Forderung des Zentralverbandes des Deutschen Handwerks lautet, dass eine Norm den am Markt verfügbaren Stand der Technik und nicht den Stand der Forschung widerspiegeln soll. [56, S. 3] Die Bedeutung des Stands der Technik ist nicht eindeutig definiert, jedoch u. a. in verschiedenen Gesetzen und Verordnungen erwähnt, so z. B. in Artikel 25 DSGVO (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen), Artikel 32 DSGVO (Sicherheit der Verarbeitung), § 8a BSIG (Sicherheit in der Informationstechnik Kritischer Infrastrukturen) und § 8c BSIG (Besondere Anforderungen an Anbieter digitaler Dienste). Vereinzelte Gesetze konkretisieren in deren Regelungsbereich den Stand der Technik. Eine Übertragbarkeit ist durch den direkten Bestimmungsbezug aber nicht möglich. Beispielsweise ist im § 3 Abs. 6 Bundes-Immissionsschutzgesetz (Begriffsbestimmungen) Folgendes geregelt:

„*(6) Stand der Technik im Sinne dieses Gesetzes ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zur Begrenzung von Emissionen in Luft, Wasser und Boden, zur Gewährleistung der Anlagensicherheit, zur Gewährleistung einer umweltverträglichen Abfallentsorgung oder sonst zur Vermeidung oder Verminderung von Auswirkungen auf die Umwelt zur Erreichung eines allgemein hohen Schutzniveaus für die Umwelt insgesamt gesichert erscheinen lässt. Bei der Bestimmung des Standes der Technik sind insbesondere die in der Anlage aufgeführten Kriterien zu berücksichtigen.*“

Die erwähnte Anlage benennt zu berücksichtigende Regelkriterien wie den Einsatz abfallarmer Technologien, die Verwendung weniger gefährlicher Stoffe, technologische Fortschritte und wissenschaftliche Erkenntnisse.

Das Bundesverfassungsgericht beschäftigte sich in seinem Urteil von 1978 mit dem Stand der Technik und dessen Abgrenzungen. Es unterscheidet:

- allgemein anerkannten Regeln der Technik,
- Stand der Technik und den
- Stand von Wissenschaft und Technik.

Die allgemein anerkannten Regeln der Technik stellen die geringste Anforderungsstufe dar. Hier reiche die Feststellung der herrschenden Auffassung der technischen Prakti-

ker. Diese Regeln hinken jedoch stets den fortschreitenden technischen Weiterentwicklungen hinterher. [67, Abs. 96] Ergänzend führt das Bundesministerium für Justiz aus, dass diese Regeln sich in der Praxis bewährt haben und für Fälle mit eher geringem Gefährdungspotential gelten. [68, Rn. 255]

Die nächste Stufe stelle der Stand der Technik dar. Der vorgenannte Nachteil wird hier vermieden. Das Bundesverfassungsrichtgericht führt hierzu aus:

„*Der rechtliche Maßstab für das Erlaubte oder Gebotene wird hierdurch an die Front der technischen Entwicklung verlagert, da die allgemeine Anerkennung und die praktische Bewährung allein für den Stand der Technik nicht ausschlaggebend sind.*“

Es betont zudem:

„*Bei der Formel vom Stand der Technik gestaltet sich die Feststellung und Beurteilung der maßgeblichen Tatsachen für Behörden und Gerichte allerdings schwieriger. Sie müssen in die Meinungsstreitigkeiten der Techniker eintreten, um zu ermitteln, was technisch notwendig, geeignet, angemessen und vermeidbar ist*“. [67, Abs. 97]

Das Bundesministerium für Justiz empfiehlt in diesem Bezug eine etwas abweichende Definition:

„*Stand der Technik ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen, der nach herrschender Auffassung führender Fachleute das Erreichen des gesetzlich vorgegebenen Zieles gesichert erscheinen lässt. Verfahren, Einrichtungen und Betriebsweisen oder vergleichbare Verfahren, Einrichtungen und Betriebsweisen müssen sich in der Praxis bewährt haben oder sollten – wenn dies noch nicht der Fall ist – möglichst im Betrieb mit Erfolg erprobt worden sein*“. [68, Rn. 256]

Aus Sicht des Deutschen Institutes für Normung wird der Stand der Technik definiert als:

„e*in entwickeltes Stadium der technischen Möglichkeiten zu einem bestimmten Zeitpunkt, soweit Produkte, Prozesse und Dienstleistungen betroffen sind, basierend auf den diesbezüglichen gesicherten Erkenntnissen von Wissenschaft, Technik und Erfahrung.*“ [17, S. 85, 37, S. 17]

Das DIN definiert die anerkannte Regel der Technik als:

„*technische Festlegung, die von einer Mehrheit repräsentativer Fachleute als Wiedergabe des Standes der Technik angesehen wird*“. [17, S. 85, 37, S. 19]

Als höchste Stufe deklariert das Bundesverfassungsgericht den Stand von Wissenschaft und Technik. Er soll am nächsten an den aktuellen wissenschaftlichen sowie rechtlichen Stand reichen. Das Gericht stellt fest:

„*Es muß diejenige Vorsorge gegen Schäden getroffen werden, die nach den neuesten wissenschaftlichen Erkenntnissen für erforderlich gehalten wird. Läßt sie sich technisch noch nicht verwirklichen, darf die Genehmigung nicht erteilt werden*“. [67, Abs. 98]

Kurz gefasst, der geforderte Stand der Technik beinhaltet fortschrittliche und allgemein verfügbare Technik, deren Einsatz verhältnismäßig ist. Uneinigkeit herrscht hinsichtlich einer notwendigen praktischen Bewährtheit oder Erprobung. Die Norm-Prüfung setzt folglich eine Fortschrittserhebung sowie einen entsprechenden Diskurs voraus.

Der letzte Aspekt in diesem Kompatibilitätskriterium ist die Forderung nach Einführung einfacher Rechenverfahren, anstelle der Beibehaltung der Referenzmethoden. Derartige Methoden sind aus der Norm herauslesbar und bedürfen keiner weiteren Überprüfungsmethode.

4.2.5 Anforderungsprüfbarkeit

Die Norm soll den konkreten Anwendungsbereich mitsamt den Grenzen definieren. Die KMU sollen klar erkennen können, welche ihrer Produkte oder Dienstleistung von der Norm umfasst werden. [57, S. 9]

Norm-Anforderungen sollen als Leistungsmerkmale ausgedrückt werden und nicht durch konstruktive oder deskriptive Merkmale. Dadurch werde ein ergebnisorientierter Ansatz unterstützt und erlaube dem technischen Fortschritt die größte Unabhängigkeit. [57, S. 8] Ferner erleichtert diese Ausdrucksweise die Prüfbarkeit der Norm-Realisierung. Das folgende Beispiel in der DIN 820-2 verdeutlicht den Unterschied:

„Gestaltungsanforderungen: Der Tisch muss vier Tischbeine aus Holz haben.

Leistungsanforderungen: Der Tisch muss so ausgeführt sein, dass er bei/unter … [Stabilitäts- und Festigkeitskriterien].“ [58, S. 53]

Die Prüfung dieses Aspekts ist durch das Lesen der Norm möglich.

4.3 Zusammenfassung Kompatibilitätskriterien

Die Prüfbarkeit der gestellten Anforderungen an Normen sind nicht bei jedem Aspekt ohne Weiteres möglich. Insbesondere die individuelleren Aspekte, wie Wirtschaftlichkeit oder Verständlichkeit, bedürfen einer verstärkten Einbindung der Norm-Zielgruppe. In der Tabelle 3 sind stichpunktartig die Kriterien mit ihren Aspekten und Prüfmethoden aufgeführt. Der Großteil der Aspekte kann durch einen Textabgleich, also durch das Lesen der Norm, unter dem Blickwinkel des jeweiligen Aspektes, geprüft werden. Diese werden im nächsten Kapitel bewertet.

Kompatibilitätskriterien	**Aspekt**	**Prüfmethode(n)**
Vollständigkeit	▪ Alle zum Themenfeld gehöriger Normen, inklusive Querschnittsnormen sind aufgelistet ▪ Die im Anwendungsbereich genannten Inhalte sind vollständig	▪ Recherche durch Normungsorganisation ▪ Textabgleich
Aufbau	▪ Erstellungsmotivation ▪ Benennung Normenziel sowie Zielgruppe ▪ gute Übersichtlichkeit ▪ relevante Informationen schnell auffindbar ▪ nachvollziehbare Versionsänderungen	▪ Textabgleich ▪ Textabgleich ▪ emp. U. ▪ Textabgleich, besser emp. U. ▪ Textabgleich

Kompatibilitätskriterien	Aspekt	Prüfmethode(n)
Lesbarkeit und Verständlichkeit	▪ leichte Lesbarkeit ▪ allgemeinverständliche Sprache ▪ Abkürzungen sind erklärt ▪ komplizierte Ausdrücke sind erklärt ▪ Vermittlung von Grundlagenwissen ▪ Nutzung von Beispielen, weiteren Erklärungen oder Veranschaulichungen ▪ Normenlänge so kurz wie nötig ▪ Vermeidung von Querverweisen innerhalb der Normen ▪ Vermeidung von Verweisungen auf andere Normen, ggf. Text zitieren ▪ deutsche Sprache ▪ Vermeidung inhaltlicher und thematischer Norm-Dopplungen	▪ FREdeutsch ▪ emp. U. ▪ Textabgleich ▪ emp. U. ▪ emp. U. ▪ Textabgleich ▪ Praktische Umsetzung ▪ Textabgleich ▪ Textabgleich ▪ Textabgleich ▪ Normenabgleich von Norm-Experten
Wirtschaftlichkeit	▪ Normen-Zugänglichkeit ▪ Verhältnismäßigkeit der entstehenden Kosten durch Normeinführung ▪ Normen spiegeln den am Markt verfügbaren Stand der Technik wider ▪ vereinfachte Rechenverfahren verwenden	▪ Online-Recherche ▪ emp. U. ▪ emp. U. ▪ Textabgleich
Prüfbarkeit der Anforderungen	▪ Definierter Anwendungsbereich ▪ Anforderungen als Leistungsmerkmale ausgedrückt	▪ Textabgleich ▪ Textabgleich

Tabelle 3: Gegenüberstellung der einzelnen Aspekte zu den Prüfmethoden auf KMU-Tauglichkeit

4.4 Bewertung

Eine Bewertung erfolgt in Punkten, anhand der im Kapitel zuvor beschriebenen Prüfmethoden. Der Vergleichsmaßstab der Punktevergabe sind die Normen und Standards untereinander. Welche den betrachteten Aspekt am ehesten erfüllt, bekommt vier Punkte, die am wenigsten erfüllt, einen Punkt. Bei Aspekten, bei denen lediglich das Vorhandensein geprüft wird, bekommt im positiven Fall ebenso vier Punkte und im negativen Fall keinen Punkt. Bei gleichem Aspekterfüllungsgrad werden die gleichen Punkte vergeben. Der Nächstniedrigere erhält Punkte in einem Umfang, als hätten zwei Normen einen besseren Erfüllungsgrad. Eine Ausnahme ist, wenn ein Aspekt mehrere Existenzprüfungen beinhaltet, in diesen Fällen werden anteilig Punkte vergeben. Eine weitere Ausnahme entsteht, wenn ein Aspekt nicht vollständig erfüllt wurde, so z. B. bei partieller Aufnahme von Abkürzungen in das Abkürzungsverzeichnis. In derartigen Fällen wird die maximale Punktzahl halbiert. Insofern der Aspekt einer Norm nicht prüfbar ist, wird dieser auch nicht in die Berechnung mit einbezogen. Anteilmäßig wird die maximal erreichbare Punktzahl gesenkt. Im Ergebnis ergibt sich aus dem prozentualen Anteil der erreichten Punktzahl von der maximal erreichbaren Gesamtpunktzahl die KMU-Tauglichkeit.

Jeder betrachtete Aspekt wird bewertet. Daraus ergibt sich eine Gewichtung der einzelnen Kompatibilitätskriterien. Das Kompatibilitätskriterium mit den meisten erreichbaren Punkten (24 Punkte) entfällt auf das Kompatibilitätskriterium Lesbarkeit und Verständlichkeit. Die niedrigste maximale Punktezahl ist mit dem Kriterium der Vollständigkeit erreichbar (4 Punkte).

Die Zuordnung der bewertbaren Aspekte und deren Punktebereiche sind in der Tabelle 4 ersichtlich. Die vollständige Auflistung, also auch mit den Aspekten, die nicht ohne Weiteres auswertbar (n. a.) sind, befindet sich in der Anlage 2.

Kompatibilitätskriterien	Aspekt	Punktebereich
Vollständigkeit	▪ Die im Anwendungsbereich genannten Inhalte sind vollständig	▪ 0, 4
Aufbau	▪ Erstellungsmotivation ▪ Benennung Normenziel sowie Zielgruppe ▪ relevante Informationen schnell auffindbar ▪ nachvollziehbare Versionsänderungen	▪ 0, 4 ▪ 0, 2, 4 ▪ 1 bis 4 ▪ 0, 4
Lesbarkeit und Verständlichkeit	▪ leichte Lesbarkeit ▪ Abkürzungen sind erklärt ▪ Nutzung von Beispielen, weiteren Erklärungen oder Veranschaulichungen ▪ Vermeidung von Querverweisen innerhalb der Normen ▪ Vermeidung von Verweisungen auf andere Normen, ggf. Text zitieren ▪ deutsche Sprache	▪ 1 bis 4 ▪ 0, 4 ▪ 1 bis 4 ▪ 1 bis 4 ▪ 1 bis 4 ▪ 0, 4
Wirtschaftlichkeit	▪ Normen-Zugänglichkeit ▪ Verhältnismäßigkeit der entstehenden Kosten durch Normeinführung ▪ vereinfachte Rechenverfahren verwenden	▪ 0, 4 ▪ 1 bis 4 ▪ 0, 4
Prüfbarkeit der Anforderungen	▪ Definierter Anwendungsbereich ▪ Anforderungen als Leistungsmerkmale ausgedrückt	▪ 0, 4 ▪ 0, 4

Tabelle 4: Übersicht der bewertbaren Aspekte und deren Punktebereiche

4.4.1 Bewertung BSI-Standard 100-4

Die im Kapitel 4 herausgearbeiteten Prüfmethoden werden im Nachfolgenden auf den BSI-Standard 100-4 angewendet.

Vollständigkeit (Bewertung 4 von 4 Punkten)

Der Anwendungsbereich ist im Kapitel 1.2 (Zielsetzung) beschrieben. In diesem Standard soll „eine Methodik zur Etablierung und Aufrechterhaltung eines behörden- bzw. unternehmensweiten internen Notfallmanagements vorgestellt“ werden. [20, S. 1] Die Kapitel 4 bis 9 beschreiben eine entsprechende Methodik, die diesen Aspekt erfüllt. *Bewertung: 4 von 4 Punkten*

Aufbau (Bewertung: 15 von 16 Punkten)

Die Motivation zur Erstellung dieses Standards ist ebenfalls im Punkt Zielsetzung aufgeführt. [20, S. 1] *Bewertung: 4 von 4 Punkten*

Das Ziel des Standards ist ebenfalls dort ausführlich beschrieben. Die Zielgruppe ist im Kapitel 1.3 (Adressatenkreis) wie folgt benannt:

„*Dieses Dokument richtet sich an Notfall- bzw. Business Continuity Manager, Krisenstabsmitglieder, Sicherheitsverantwortliche, -beauftragte, -experten und -berater, die mit dem Management von Notfällen und Krisen technischen und nicht-technischen Ursprungs betraut sind. Anwender der in diesem Dokument beschriebenen Methodik sollten mit der IT-Grundschutz-Vorgehensweise, die im BSI-Standard 100-2 beschrieben ist, vertraut sein.*“ [20, S. 2] *Bewertung: 4 von 4 Punkten*

Hinweise auf eine schnelle Auffindbarkeit relevanter Information geben ein Inhalts- sowie Stichwortverzeichnis und Kurzbeschreibungen der Kapitel mit Zielsetzung. Im vorliegenden Standard ist ein Inhaltsverzeichnis vorhanden. Ein Glossar ist auf den Seiten 100 und 101 vorhanden. Die Kapitel beginnen mit einer Kurzbeschreibung. Die Zielsetzung der jeweiligen Kapitel geht jedoch überwiegend nicht oder nicht prägnant hervor. *Bewertung: 3 von 4 Punkten*

Die Versionsänderungen sollen nachvollziehbar sein. Das erste Unterkapitel in lautet „Versionshistorie“ [20, S. 1]. Dort ist bereits der erste und einzige Versionsstand eingetragen. *Bewertung: 4 von 4 Punkten*

Lesbarkeit und Verständlichkeit (Bewertung 15 von 24 Punkten)

Laut der Webseite http://textinspektor.de/text_testen2.php5 enthält der eingelesene Standard 2.744 Sätze, 44.416 Wörter und 104.378 Silben. Daraus ergeben sich eine durchschnittliche Satzlänge (ASL) von 16,19 Wörtern pro Satz und 2,35 Silben pro Wort (ASW). Auszüge befinden sich in den Anlagen 2 und 3. Der angewendete Flesch-Reading-Ease (für deutschsprachige Texte) beträgt 26,34. Der Text zählt damit nach der Flesch-Lesbarkeitseinteilung zu den eher sehr schwer lesbaren Texten. *Bewertung: 3 von 4 Punkten*

$$FRE_{deutsch} = 180 - 16{,}19 - (58{,}5 \bullet 2{,}35) = 26{,}34$$

Formel 4: Flesch-Reading-Ease für deutschsprachige Texte auf BSI-Standard 100-4 angewendet

Im betrachteten BSI-Standard werden Abkürzungen definiert und verwendet, so. z. B. ISMS auf Seite 4, jedoch gibt es kein Abkürzungsverzeichnis. *Bewertung: 2 von 4 Punkten.*

In dem Standard sind zahlreiche Beispiele und weiteren Erklärungen zu finden, z. B. im Anhang A. Auf den 117 nummerierten Seiten befinden sich inklusive Glossar 20 Tabellen und 12 Abbildungen. *Bewertung: 4 von 4 Punkten*

Innerhalb des Standards werden 26 Querverweise mit dem Wort „siehe“ eingeleitet. Es wird hauptsächlich auf Kapitel, Tabellen und Abbildungen verwiesen. *Bewertung: 1 von 4 Punkten*

Verweisungen auf andere Standards und Normen sind insb. im Rahmen der Einleitung und Einordnung in andere BSI-Standards sowie der Beschreibung anderer Notfallmanagement-Standards auffindbar. Allerdings auch an diversen anderen Stellen. Das Literaturverzeichnis umfasst 21 Punkte zu anderen Standards, Normen und Leitfäden. *Bewertung: 1 von 4 Punkten*

Der BSI-Standard ist in deutscher Sprache verfasst. *Bewertung: 4 von 4 Punkten*

Wirtschaftlichkeit (Bewertung 12 von 12 Punkten)

Die Norm ist über die Webseite des BSI (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1004.pdf?__blob=publicationFile&v=2) abrufbar. *Bewertung: 4 von 4 Punkten*

Der Standard ist kostenlos herunterladbar. *Bewertung: 4 von 4 Punkten*

Die enthaltenen Berechnungsmodelle, insb. in der Business-Impact-Analyse, sind eher einfache Rechenverfahren. *Bewertung: 4 von 4 Punkten*

Prüfbarkeit der Anforderungen (Bewertung 8 von 8 Punkten)

Der Standard definiert im Kapitel der Einleitung, insb. im Kapitel 1.2 (Zielsetzung) sowie im Kapitel 1.4 (Anwendungsweise) den konkreten Anwendungsbereich mitsamt den Grenzen. *Bewertung: 4 von 4 Punkten*

Die Anforderung Leistungsmerkmale zu verwenden ist erfüllt. Es werden zumeist Auflistungen von Kriterien angegeben, die geprüft oder berücksichtigt werden sollen. So sind exemplarisch im Risikoanalyse-Bericht Inhalte, wie z. B. die verwendete Methode, Liste der Risiken und die Ergebnisse der Risikobewertung, aufgelistet. *Bewertung: 4 von 4 Punkten*

Ergebnis

Aus den Bewertungen resultiert die folgende Gesamtpunktzahl: 54 von 64 von Punkten. Die KMU-Tauglichkeit beträgt 84,38 %.

4.4.2 Bewertung B3S Gesundheit

Die im Kapitel 4 herausgearbeiteten Prüfmethoden werden im Nachfolgenden auf den B3S Gesundheit angewendet.

Vollständigkeit (Bewertung 2 von 4 Punkten)

Der Anwendungsbereich ist nicht im ersten Kapitel beschrieben. Es werden zuerst Beschreibungen und Begründungen zur B3S-Erstellung geben sowie gesetzliche Regelungen aufgegriffen. Im Kapitel 2 werden ebenfalls Ausführungen zur B3S-Erstellung vorgenommen. Erst im Kapitel 3.1 (Grundlegendes zur Anwendung des B3S) ist der Anwendungsbereich beschrieben. Mit dem B3S Gesundheit werde „eine geeignete Prüfgrundlage zum Umsetzungsnachweis der erforderlichen Maßnahmen“ hinsichtlich der Umsetzanforderungen nach § 8a Abs. 1 BSIG gegeben [22, S. 11]. Da das BSI die Geeignetheit bereits festgestellt hat [21], gilt dieser Aspekt dahingehend als erfüllt. Allerdings ist dieser nicht im Vorwort bzw. der Einleitung erfasst, daher werden Punkte abgezogen. *Bewertung: 2 von 4 Punkten*

Aufbau (Bewertung: 9 von 16 Punkten)

Die Motivation zur Erstellung dieses Standards geht nicht klar hervor. Es finden sich Hinweise im Kapitel 1 (Vorwort) und Kapitel 3 (Branchenspezifischer Sicherheitsstandard (B3S) für die medizinische Versorgung) [22, S. 6–11]. Daher erfolgt auch hier ein Punktabzug. *Bewertung: 2 von 4 Punkten*

Das Ziel des Standards ist im Kapitel 1.3 (Branchenspezifische Sicherheitsstandards (B3S) benannt und die Zielgruppe in Kapitel 1.4 (Kritische Infrastrukturen in der Branche „Medizinische Versorgung“) aufgeführt. *Bewertung: 4 von 4 Punkten*

Hinweise auf eine schnelle Auffindbarkeit relevanter Information geben ein Inhalts- sowie Stichwortverzeichnis und Kurzbeschreibungen der Kapitel mit Zielsetzung. Im vorliegenden Standard ist ein Inhaltsverzeichnis vorhanden. Ein Glossar ist auf den Seiten 87 und 88 vorhanden. Die Kapitel beginnen mit einer Kurzbeschreibung. Die Zielsetzung der jeweiligen Kapitel geht jedoch überwiegend nicht oder nicht prägnant hervor. Bewertung: *3 von 4 Punkten*

Die Versionsänderungen sollen nachvollziehbar sein. Eine Versionshistorie ist nicht vorhanden, obwohl es sich bereits um Version 1.1 handelt. Auch ein Platzhalter ist für zukünftige nicht existent. *Bewertung: 0 von 4 Punkten*

Lesbarkeit und Verständlichkeit (Bewertung 17 von 24 Punkten)

Laut der Webseite http://textinspektor.de/text_testen2.php5 enthält der eingelesene Standard 1.849 Sätze, 24.009 Wörter und 58.822 Silben. Daraus ergeben sich eine durchschnittliche Satzlänge (ASL) von 12,98 Wörtern pro Satz und 2,45 Silben pro Wort (ASW). Der angewendete Flesch-Reading-Ease (für deutschsprachige Texte) beträgt 23,7. Der Text zählt damit nach der Flesch-Lesbarkeitseinteilung zu den eher sehr schwer lesbaren Texten. *Bewertung: 2 von 4 Punkten*

$$FRE_{deuts} = 180 - 12{,}98 - (58{,}5 \bullet 2{,}45) = 23{,}7$$

Formel 5: Flesch-Reading-Ease für deutschsprachige Texte auf den Standard B3S Gesundheit angewendet

Im betrachteten BSI-Standard werden Abkürzungen definiert und verwendet, so. z. B. kDL für kritische Dienstleistungen auf Seite 9, jedoch gibt es kein Abkürzungsverzeichnis. *Bewertung: 2 von 4 Punkten.*

In dem Standard sind viele Beispiele und weiteren Erklärungen zu finden, z. B. in der Risikodefinition. Auf den 88 nummerierten Seiten befinden sich 1 Tabellen und 5 Abbildungen. Die Nummerierungen fehlen allerdings teilweise. *Bewertung: 3 von 4 Punkten*

Innerhalb des Standards werden 5 Querverweise mit dem Wort „siehe“ eingeleitet. *Bewertung: 3 von 4 Punkten*

Verweisungen auf andere Standards und Normen sind insb. im Rahmen des ersten Kapitels auffindbar. Das Verzeichnis auf referenzierte Normen und Standards umfasst sieben Einträge. *Bewertung: 3 von 4 Punkten*

Der betrachtete Standard ist in deutscher Sprache verfasst. *Bewertung: 4 von 4 Punkten*

Wirtschaftlichkeit (Bewertung 8 von 12 Punkten)

Die Norm ist online unter https://www.dkgev.de/fileadmin/default/Mediapool/2_Themen/2.1_Digitalisierung_Daten/2.1.4._IT-Sicherheit_und_technischer_Datenschutz/2.1.4.1._IT-Sicherheit_im_Krankenhaus/B3S_KH_v1.1_8a_geprueft.pdf abrufbar.

Bewertung: 4 von 4 Punkten

Der Standard ist kostenlos herunterladbar. *Bewertung: 4 von 4 Punkten*

Es sind keine Berechnungsmodelle enthalten, obwohl an verschiedenen Stellen eine Messbarkeit erwartbar ist. So beispielsweise bei der Bewertung von Risiken (Eintrittswahrscheinlichkeit und Schadenspotential). *Bewertung: 0 von 4 Punkten*

Prüfbarkeit der Anforderungen (Bewertung 8 von 8 Punkten)

Der Standard definiert insb. im Kapitel 3.1 (Grundlegendes zur Anwendung des B3S) den konkreten Anwendungsbereich. *Bewertung: 4 von 4 Punkten*

Die Anforderung Leistungsmerkmale zu verwenden ist erfüllt. Es werden zumeist Auflistungen von Kriterien angegeben, die geprüft oder berücksichtigt werden sollen. *Bewertung: 4 von 4 Punkten*

Ergebnis

Aus den Bewertungen resultiert die folgende Gesamtpunktzahl: 44 von 64 von Punkten. Die KMU-Tauglichkeit beträgt 68,75 %.

4.4.3 Bewertung DIN EN ISO/IEC ISO 27001

Die im Kapitel 4 herausgearbeiteten Prüfmethoden werden im Nachfolgenden auf die Norm DIN EN ISO/IEC ISO 27001:2017-06 angewendet.

Vollständigkeit (Bewertung 4 von 4 Punkten)

Der Anwendungsbereich ist im Kapitel 1 wie folgt beschrieben:

„*Diese Internationale Norm legt die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Informationssicherheitsmanagementsystems im Kontext der Organisation fest. Darüber hinaus beinhaltet diese Internationale Norm Anforderungen für die Beurteilung und Behandlung von Informationssicherheitsrisiken entsprechend den individuellen Bedürfnissen der Organisation.*“ [33, S. 6] Die Kapitel 4 bis 10 beschreiben entsprechende Anforderungen. *Bewertung: 4 von 4 Punkten*

Aufbau (Bewertung: 13 von 16 Punkten)

Die Motivation zur Erstellung dieser Norm ist im Kapitel 0.1 (Allgemeines) aufgeführt. [20, S. 1] *Bewertung: 4 von 4 Punkten*

Das Normziel ist ebenfalls dort prägnant beschrieben. Die Zielgruppe ist im Kapitel 1 (Anwendungsbereich) wie folgt benannt:

„*Die in dieser Internationalen Norm festgelegten Anforderungen sind allgemein gehalten und sollen auf alle Organisationen, ungeachtet ihrer Art und Größe, anwendbar sein.*“ [33, S. 6] *Bewertung: 4 von 4 Punkten*

Hinweise auf eine schnelle Auffindbarkeit relevanter Information geben ein Inhalts- sowie Stichwortverzeichnis und Kurzbeschreibungen der Kapitel mit Zielsetzung. Im vorliegenden Standard ist ein Inhaltsverzeichnis vorhanden. Ein Stichwortverzeichnis oder Glossar ist nicht vorhanden, ebenso wenig eine Kapiteleinleitung mit Kurzbeschreibung sowie Zielsetzung. *Bewertung: 1 von 4 Punkten*

Die Versionsänderungen sollen nachvollziehbar sein. Im Bereich des nationalen Vorwortes, im Punkt „Änderungen“, sind diese beschrieben [33, S. 2]. *Bewertung: 4 von 4 Punkten*

Lesbarkeit und Verständlichkeit (Bewertung 17 von 24 Punkten)

Nach Angaben der Webseite http://textinspektor.de/text_testen2.php5 enthält die eingelesene Norm 747 Sätze, 6.870 Wörter und 17.725 Silben. Daraus ergeben sich eine durchschnittliche Satzlänge (ASL) von 9,20 Wörtern pro Satz und 2,58 Silben pro Wort (ASW). Der angewendete Flesch-Reading-Ease (für deutschsprachige Texte) beträgt 19,87. Der Text zählt damit nach der Flesch-Lesbarkeitseinteilung zu den sehr schwer lesbaren Texten. *Bewertung: 1 von 4 Punkten*

$$FRE_{deutsch} = 180 - 9{,}20 - (58{,}5 \bullet 2{,}58) = 19{,}87$$

Formel 6: Flesch-Reading-Ease für deutschsprachige Texte auf DIN EN ISO/IEC 27001 angewendet

In der betrachteten Norm werden Abkürzungen definiert und verwendet, so. z. B. ISMS auf Seite 5, jedoch gibt es kein Abkürzungsverzeichnis. *Bewertung: 2 von 4 Punkten.*

Die Norm verwendet lediglich ein ausgewiesenes Beispiel. Auf den 31 nummerierten Seiten befinden sich eine Tabelle (Anhang A) und keine Abbildungen. *Bewertung: 2 von 4 Punkten*

Innerhalb der Norm werden zwei Querverweise mit dem Wort „siehe“ eingeleitet. *Bewertung: 4 von 4 Punkten*

Verweisungen auf andere Standards und Normen sind konzentrierter in der Einleitung auffindbar. Die Literaturhinweise beinhalten sechs Normen. *Bewertung: 4 von 4 Punkten*

Die Norm ist in deutscher Sprache verfasst. *Bewertung: 4 von 4 Punkten*

Wirtschaftlichkeit (Bewertung 6 von 12 Punkten)

Die Norm ist über die Webseite des Beuth Verlages (https://www.beuth.de/de/norm/din-en-iso-iec-27001/269670716) abrufbar. *Bewertung: 4 von 4 Punkten*

Der Norm kostet brutto im Portable Document Format (PDF) 92,74 Euro, mit Stand vom 31.07.2020. *Bewertung: 2 von 4 Punkten*

Es sind keine Berechnungsmodelle enthalten, obwohl an verschiedenen Stellen eine Messbarkeit erwartbar ist. So beispielsweise bei der Bewertung von Eintrittswahrscheinlichkeiten von Informationssicherheitsrisiken. *Bewertung: 0 von 4 Punkten*

Prüfbarkeit der Anforderungen (Bewertung 8 von 8 Punkten)

Die Norm definiert im Kapitel 1 den konkreten Anwendungsbereich. Eine Grenzsetzung erfolgt nicht. *Bewertung: 4 von 4 Punkten*

Die Anforderung Leistungsmerkmale zu verwenden ist erfüllt. Es werden zumeist Auflistungen von Kriterien angegeben, die geprüft oder berücksichtigt werden sollen, insb. im Anhang A. *Bewertung: 4 von 4 Punkten*

Ergebnis

Aus den Bewertungen resultiert die folgende Gesamtpunktzahl: 48 von 64 von Punkten. Die KMU-Tauglichkeit beträgt 75 %.

4.4.4 Bewertung DIN EN ISO 22301

Die im Kapitel 4 herausgearbeiteten Prüfmethoden werden im Nachfolgenden auf die Norm DIN EN ISO 22301:2020-06 angewendet.

Vollständigkeit (Bewertung 4 von 4 Punkten)

Der Anwendungsbereich ist im Kapitel 1 wie folgt beschrieben:

„*Dieses Dokument legt Anforderungen fest, um ein Managementsystem zu verwirklichen, aufrechtzuerhalten und zu verbessern, um sich gegen Störungen zu schützen, die Wahrscheinlichkeit ihres Auftretens zu vermindern, sich auf diese vorzubereiten, auf diese zu reagieren und sich von diesen zu erholen, wann immer sie auftreten.*“ [44, S. 10] Die Kapitel 4 bis 10 beschreiben entsprechende Anforderungen. *Bewertung: 4 von 4 Punkten*

Aufbau (Bewertung: 16 von 16 Punkten)

Die Motivation zur Erstellung dieser Norm ist im Kapitel 0.1 (Allgemeines) aufgeführt. *Bewertung: 4 von 4 Punkten*

Das Normziel ist ebenfalls dort prägnant beschrieben. Die Zielgruppe ist im Kapitel 1 (Anwendungsbereich) wie folgt angegeben:

„*Die in diesem Dokument aufgeführten Anforderungen sind allgemeiner Art und dafür vorgesehen, für sämtliche Organisationen oder Teile dieser, unabhängig von ihrer Art,*

Größe oder Beschaffenheit zu gelten. Der Umfang der Anwendung dieser Anforderungen ist von der betrieblichen Umgebung und der Komplexität der jeweiligen Organisation abhängig.“ [44, S. 10] *Bewertung: 4 von 4 Punkten*

Hinweise auf eine schnelle Auffindbarkeit relevanter Information geben ein Inhalts- sowie Stichwortverzeichnis und Kurzbeschreibungen der Kapitel mit Zielsetzung. Im vorliegenden Standard ist ein Inhaltsverzeichnis vorhanden. Eine Definitionsübersicht verwendeter Begriffe ist im Kapitel 3 (Begriffe) vorhanden. Darüber hinaus befinden sich Kurzbeschreibungen der Abschnitte im Kapitel 0.3 (Planen-Durchführen-Prüfen-Handeln-Zyklus (PDCA-Zyklus)). Einzeln ausgewiesene Abschnittszielsetzungen sind nicht ersichtlich. *Bewertung: 4 von 4 Punkten*

Die Versionsänderungen sollen nachvollziehbar sein. Im Bereich des nationalen Vorwortes, im Punkt „Änderungen“, sind diese beschrieben [44, S. 2]. *Bewertung: 4 von 4 Punkten*

Lesbarkeit und Verständlichkeit (Bewertung 16 von 24 Punkten)

Nach Angaben der Webseite http://textinspektor.de/text_testen2.php5 enthält die eingelesene Norm 511 Sätze, 7.870 Wörter und 17.865 Silben. Daraus ergeben sich eine durchschnittliche Satzlänge (ASL) von 15,40 Wörtern pro Satz und 2,27 Silben pro Wort (ASW). Der Flesch-Reading-Ease (deutschsprachige Texte) beträgt 31,8. Der Text zählt damit nach der Flesch-Lesbarkeitseinteilung zu den eher schwer lesbaren Texten. *Bewertung: 4 von 4 Punkten*

$$FRE_{deutsch} = 180 - 15{,}4 - (58{,}5 \bullet 2{,}27) = 31{,}8$$

Formel 7: Flesch-Reading-Ease für deutschsprachige Texte auf DIN EN ISO 22301 angewendet

In der betrachteten Norm werden Abkürzungen definiert und verwendet, so. z. B. BCMS auf Seite 6, jedoch gibt es kein Abkürzungsverzeichnis. *Bewertung: 2 von 4 Punkten.*

Die Norm verwendet ein halbes Duzend ein ausgewiesene Beispiele. Unter den 34 numerierten Seiten befindet sich weder eine Tabelle noch eine Abbildungen. *Bewertung: 1 von 4 Punkten*

Innerhalb der Norm werden fünf Querverweise mit dem Wort „siehe“ eingeleitet. *Bewertung: 3 von 4 Punkten*

Verweisungen auf andere Normen sind vorrangig im Kapitel 3 (Begriffe) auffindbar. Die Literaturhinweise umfassen 17 angegebene Normen. *Bewertung: 2 von 4 Punkten*

Die Norm ist in deutscher Sprache verfasst. *Bewertung: 4 von 4 Punkten*

Wirtschaftlichkeit (Bewertung 5 von 8 Punkten)

Die Norm ist über die Webseite des Beuth Verlages (https://www.beuth.de/de/norm/din-en-iso-22301/311095091) abrufbar. *Bewertung: 4 von 4 Punkten*

Der Norm kostet brutto als PDF 97,93 Euro, mit Stand vom 31.07.2020. *Bewertung: 1 von 4 Punkten*

Es sind keine Berechnungsmodelle enthalten und werden auch nicht deutlich indirekt angesprochen. *Keine Bewertung*

Prüfbarkeit der Anforderungen (Bewertung 8 von 8 Punkten)

Die Norm definiert im erforderlichen Maß im Kapitel 1 den konkreten Anwendungsbereich. *Bewertung: 4 von 4 Punkten*

Die Anforderung Leistungsmerkmale zu verwenden ist erfüllt. Es werden zumeist Auflistungen von Kriterien angegeben, die geprüft oder berücksichtigt werden sollen. *Bewertung: 4 von 4 Punkten*

Ergebnis

Aus den Bewertungen resultiert die folgende Gesamtpunktzahl: 49 von 60 Punkten. Die KMU-Tauglichkeit beträgt 81,67 %.

4.4.5 Gesamtergebnis

Die vorgenannten Normen und Standards wurden auf ihre KMU-Tauglichkeit geprüft. Hierbei wurden auf die Kompatibilitätskriterien Vollständigkeit, Aufbau, Lesbarkeit und Verständlichkeit, Wirtschaftlichkeit und Prüfbarkeit der Anforderungen bewertet. Die höchste KMU-Tauglichkeit mit 84,38% weißt der BSI-Standard 100-4 auf, damit sollte dieser am ehesten von KMU verwendet werden. Mit 81,67 % folgt die DIN EN ISO 22301. Auf Rang drei befindet sich die DIN EN ISO/IEC 27001 mit 75 %. Die niedrigste KMU-Tauglichkeit mit 68,75 % hat der B3S Gesundheit. Die geprüften Normen und Standards erfüllen im Ergebnis überwiegend die gestellten Anforderungen. Die Standards bilden den besten und niedrigsten Platz in der Rangliste ab. Die beiden Normen das Mittelfeld. Das Kompatibilitätskriterium Prüfbarkeit der Anforderungen ist in allen Fällen voll erfüllt. Hinsichtlich des Kompatibilitätskriteriums Lesbarkeit und Verständlichkeit besteht der größte Verbesserungsbedarf. Eine Ergebnisübersicht befindet sich in Tabelle 5.

5 Zusammenfassung

Eine unzureichende unternehmerische Vorbereitung kann im Ernstfall existenzbedrohend sein. [69] Dies wird aktuell im Kontext der COVID-19-(Corona-)Pandemie deutlich. Auch wenn noch keine belastbaren Zahlen zu Unternehmensinsolvenzen in Deutschland durch diese Pandemie vorliegen, wird bereits mit starken Auswirkungen auf Unternehmen gerechnet. Die norddeutschen Industrie- und Handelskammern haben in diesem Zusammenhang eine Umfrage mit Unternehmen in Ihrem Zuständigkeitsbereich durchgeführt und Ende März 2020 veröffentlicht. Von den ca. 4.500 antwortenden Unternehmen sehen sich 17,6 % von Insolvenz bedroht. 46,7 % meldeten demnach einen großteiligen oder kompletten Stillstand der geschäftlichen Tätigkeiten. Mehr als jedes dritte Unternehmen (37,3 %) hat Personal abgebaut. [70, S. 3] Auch IT-Unternehmen sind von den national und international ergriffenen Maßnahmen vielfältig betroffen. Beispielsweise wurden alle Geschäfte des Unternehmens Apple Inc. sowie die der Vertriebspartner (Produzenten) zeitweise geschlossen. [71]

Die Aufrechterhaltung des Normalbetriebs eines Unternehmens ist von großer Wichtigkeit. Ereignisse, die den Betriebsablauf stören, können zu größeren Schäden führen. Folglich sollten Unternehmen sich umfangreich vorbereiten. [69] Wie derartige Vorbereitungen gestaltet werden können und welche Maßnahmen noch empfehlenswert sind, sind Gegenstand verschiedener nationalen und internationalen Standards sowie Normen. Hierbei ist zu beachten, dass diese nicht in Gänze aufeinander abgestimmt sind. Dadurch gibt es in einzelnen Bereichen Dopplungen oder Überschneidungen.

Ein KMU kann aufgrund von verschiedenen Verpflichtungen angehalten sein, ein IT-Notfallmanagement einzuführen. Dies hängt grundsätzlich vom Unternehmensgegenstand sowie der Unternehmensgröße ab. Verpflichtungen können sich zum Beispiels aus dem HGB, dem GmbHG oder der DSGVO. Eine Nachweisverpflichtung zur Einführung eines Notfallmanagements obliegt Betreibern kritischer Infrastrukturen.

Wenn ein KMU den Bedarf einer (IT-)Notfallmanagement-Einführung erkennt, steht es vor einer größeren Auswahl an etablierten Standards und Normen. Insofern eine Verpflichtung zur Implementierung besteht, sollte geprüft werden, welche Anforderungen an das Notfallmanagement gestellt werden und ob die Geeignetheit vom BSI festgestellt worden sein muss. Die Europäische Union sowie der Deutsche Handwerksverband haben erkannt, dass es Norm-Umsetzungsschwierigkeiten von KMU gibt. Daraus haben sie Anforderungen formuliert. In dieser Arbeit sind diese Grundlage für die entwickelte Methode zur KMU-Tauglichkeitsprüfung. Die auf die folgenden bekannten Standards und Normen wurde die KMU-Tauglichkeitsprüfung angewendet: BSI-Standard 100-4, B3S Gesundheit, ISO 27001 sowie die ISO 22301. Im Ergebnis hat der BSI-Standard

100-4 eine KMU-Tauglichkeit von 84,38 % erreicht und weißt damit die höchste Kompatibilität zu KMU auf. Nachfolgend sind die DIN EN ISO 22301 (81,67 %), DIN EN ISO/IEC 27001 (75 %) und der B3S Gesundheit mit 68,75 %. Im Ergebnis empfiehlt sich in diesem Rahmen am ehesten eine Einführung des BSI 100-4 Standards für KMU. Eine zusammenfassende Übersicht der Ergebnisse befindet sich in Tabelle 5.

Kompatibilitäts-kriterien	**BSI 100-4**	**B3S Gesund-heit**	**ISO 27001**	**ISO 22301**
Vollständigkeit	4 von 4	2 von 4	4 von 4	4 von 4
Aufbau	15 von 16	9 von 16	13 von 16	16 von 16
Lesbarkeit und Verständlichkeit	15 von 24	17 von 24	17 von 24	16 von 24
Wirtschaftlichkeit	12 von 12	8 von 12	6 von 12	5 von 8
Prüfbarkeit der Anforderungen	8 von 8	8 von 8	8 von 8	8 von 8
Ergebnis	54 von 64	44 von 64	48 von 64	49 von 60
KMU-Tauglichkeit	84,38 %	68,75 %	75 %	81,67 %

Tabelle 5: Entscheidungsmatrix der Kompatibilitätsbewertungen in Punkten, grau eingefärbt sind die höchsten Werte

6 Ausblick

Diese Arbeit hat die Verpflichtung zur Einführung eines IT-Notfallmanagements betrachtet und die Notwendigkeit einer KMU-Tauglichkeitsprüfung sowie deren Anforderungen dargestellt. Diese Arbeit kann unterstützen, um weitere Normen und Standards auf KMU-Tauglichkeit zu prüfen.

Es wurden nicht alle erarbeiteten Aspekte in die Bewertung mit einbezogen. Das lag u. a. an einerseits unzureichend konkretisierten Maßstäbe (z. B. zum Aspekt gute Übersichtlichkeit) und andererseits an fehlenden empirischen Untersuchungen. Des Weiteren wurde die Gewichtung bei allen Aspekten auf bis zu vier Punkten gesetzt. Damit sind im Kompatibilitätskriterium Lesbarkeit und Verständlichkeit die meisten bewertbaren Aspekte (Gesamtanteil 37,5 %) enthalten. Dieses Kriterium ist dadurch so gewichtig, wie die Kompatibilitätskriterien Vollständigkeit, Wirtschaftlichkeit und Prüfbarkeit der Anforderungen zusammen.

Ein besonderes Augenmerk könnten Untersuchungen der Lesbarkeit einnehmen. Die betrachteten Standards und Normen wurden nach dem Flesch-Reading-Ease für deutschsprachige Texte als mindestens schwer lesbar eingestuft.

Ebenfalls könnte die Bereitstellungsart hinsichtlich der KMU-Tauglichkeit geprüft werden. Die elektronische Bereitstellung der Dokumente als PDF ermöglicht eine gute Verfügbarkeit, jedoch ist fraglich, ob die Lesbarkeit und Verständlichkeit nicht durch eine andere Bereitstellungsform verbessert werden kann. Vorstellbar ist z. B. ein Software Guide, welcher den Anwender schrittweise durch die einzelnen Anforderungen führt und nur die Informationen anzeigt, die im jeweiligen Abschnitt benötigt werden. Dadurch könnten zusätzliche Normbereitstellungen, beispielsweise für einen Vokabularkatalog, wie die DIN EN ISO 22300, und das ggf. Hin- und Herblättern entfallen.

Allen aufgeführten Punkten ist die Verbesserung der Standard- und Normanwendung immanent. Insbesondere im Bereich des (IT-)Notfallmanagement können Fehler in der Umsetzung gravierende Auswirkungen haben und sollten daher einem ständigen Prüfungsprozess unterliegen. Darüber hinaus könnte sich ein noch nicht genannter, aber wichtiger Vorteil ergeben. Aus weiteren Verbesserungen könnte die Akzeptanz zur Einführung steigen und daran anknüpfend auch häufigere Umsetzungen.

Literaturverzeichnis

[1] Deutsches Institut für Normung e. V., DIN 820 Beiblatt 3: Normungsarbeit; Beiblatt 3: Hinweise und Informationen für das Erstellen, Veröffentlichen und Anwenden von Normen. Berlin: Beuth Verlag GmbH, 2016.

[2] Ministerium der Finanzen und für Europa des Landes Brandenburg, Die elektronische Steuererklärung: Was ist ELSTER? [Online] Verfügbar unter: https://mdfe.brandenburg.de/cms/detail.php/lbm1.c.392834.de. Zugriff am: Jul. 31 2020.

[3] Bundesministerium für Gesundheit, Die elektronische Patientenakte (ePA). [Online] Verfügbar unter: https://www.bundesgesundheitsministerium.de/service/begriffe-von-a-z/e/elektronische-patientenakte.html. Zugriff am: Jul. 31 2020.

[4] Bundesministerium des Innern, für Bau und Heimat, Onlinezugangsgesetz (OZG). [Online] Verfügbar unter: https://www.bmi.bund.de/DE/themen/moderne-verwaltung/verwaltungsmodernisierung/onlinezugangsgesetz/onlinezugangsgesetz-node.html. Zugriff am: Jul. 31 2020.

[5] Deutscher Industrie- und Handelskammertag, Wachsende Herausforderungen treffen auf größeren Optimismus. [Online] Verfügbar unter: https://www.karlsruhe.ihk.de/blueprint/servlet/resource/blob/2451906/9acb514a77ed9c8b661788875fe6c4d9/ihk-unternehmensbarometer-digitalisierung-data.pdf. Zugriff am: Jul. 31 2020.

[6] Bitkom e. V., Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien, Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt: Studienbericht 2020. [Online] Verfügbar unter: https://www.bitkom.org/sites/default/files/2020-02/200211_bitkom_studie_wirtschaftsschutz_2020_final.pdf. Zugriff am: Jul. 31 2020.

[7] Statista GmbH, Unternehmen in Deutschland: Anzahl der rechtlichen Einheiten* in Deutschland nach Beschäftigtengrößenklassen im Jahr 2018. [Online] Verfügbar unter: https://de.statista.com/statistik/daten/studie/1929/umfrage/unternehmen-nach-beschaeftigtengroessenklassen/. Zugriff am: Jul. 31 2020.

[8] Bundesanzeiger Verlag GmbH; Deutschland, IT-Grundschutz-Kompendium. Köln: Reguvis Bundesanzeiger Verlag; Bundesanzeiger Verlag, 2020.

[9] BITKOM, Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien, Kompass der IT-Sicherheitsstandards: Leitfaden und Nachschlagewerk. [Online] Verfügbar unter: https://www.konstanz.ihk.de/blueprint/servlet/resource/blob/4000014/02c6d5b36e71e6ec0af02d1f66346521/kompass-der-it-sicherheitsstandards-data.pdf. Zugriff am: Jul. 31 2020.

[10] Deutsches Institut für Normung e. V., DIN - kurz erklärt: Was ist eine Norm? [Online] Verfügbar unter: https://www.din.de/de/ueber-normen-und-standards/basiswissen. Zugriff am: Jul. 31 2020.

[11] A. Heidenreich, Hg., Kleines 1x1 der Normung: Ein praxisorientierter Leitfaden für KMU. Berlin: DIN [u.a.], 2010.

[12] E. Gutenberg, Einführung in die Betriebswirtschaftslehre. Wiesbaden: Gabler Verlag, 1958.

[13] Europäische Kommission, Horizon 2020 in brief: The EU framework programme for research & innovation. Luxembourg: Publications Office of the European Union, 2014.

[14] Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (Text von Bedeutung für den EWR) (Bekannt gegeben unter Aktenzeichen K(2003) 1422): Amtsblatt Nr. L 124 vom 20/05/2003 S. 0036 - 0041, (2003/361/EG), 2003.

[15] M. Stemmer und G. Goldacker, STANDARDISIERUNG FÜR DIE ÖFFENTLICHE IT, 1. Aufl. Berlin: Kompetenzzentrum Öffentliche IT, Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS, 2014.

[16] M. Klotz, Regelwerke der IT-Compliance - Klassifikation und Übersicht, Teil 2: Normen. [Online] Verfügbar unter: https://www.econstor.eu/bitstream/10419/88419/1/773961380.pdf. Zugriff am: Jul. 31 2020.

[17] DIN Deutsches Institut für Normung e. V., Hg., Normung und Standardisierung: Grundlagen, 1. Aufl. Berlin, Wien, Zürich: Beuth Verlag GmbH, 2009.

[18] K. Beckert, De Facto Standards in Information Systems: Definition & Overview. [Online] Verfügbar unter: https://study.com/academy/lesson/de-facto-standards-in-information-systems-definition-lesson-quiz.html. Zugriff am: Jul. 31 2020.

[19] DATACOM Buchverlag GmbH, De-facto-Standard. [Online] Verfügbar unter: https://www.itwissen.info/De-facto-Standard-de-facto-standard.html. Zugriff am: Jul. 31 2020.

[20] Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 100-4: Notfallmanagement. [Online] Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1004.pdf?__blob=publicationFile&v=2. Zugriff am: Jul. 31 2020.

[21] Bundesamt für Sicherheit in der Informationstechnik, BSI erkennt Cyber-Sicherheitsstandard für Krankenhäuser an. [Online] Verfügbar unter: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/B3S-Krankenhaeuser_231019.html. Zugriff am: Jul. 31 2020.

[22] Deutsche Krankenhaus Gesellschaft, Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus: Gesamtdokument. [Online] Verfügbar unter: https://www.dkgev.de/fileadmin/default/Mediapool/2_Themen/2.1_Digitalisierung_Daten/2.1.4._IT-Sicherheit_und_technischer_Datenschutz/2.1.4.1._IT-Sicherheit_im_Krankenhaus/B3S_KH_v1.1_8a_geprueft.pdf. Zugriff am: Jul. 31 2020.

[23] Bundesamt für Sicherheit in der Informationstechnik, Glossar der Cyber-Sicherheit. [Online] Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html. Zugriff am: Jul. 31 2020.

[24] Bundesamt für Sicherheit in der Informationstechnik, Fragen und Antworten zu Aufgaben und Themen des BSI. [Online] Verfügbar unter: https://www.bsi.bund.de/SharedDocs/FAQs/DE/BSI/faq_node.html. Zugriff am: Jul. 31 2020.

[25] Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kompendium – Werkzeug für Informationssicherheit. [Online] Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html. Zugriff am: Jul. 31 2020.

[26] Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS), 1. Aufl. Bonn: Bundesamt für Sicherheit in der Informationstechnik, 2017.

[27] Bundesamt für Sicherheit in der Informationstechnik, Lerneinheit 2.9: Wahl der Vorgehensweise. [Online] Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/OnlinekursITGrundschutz2018/Lektion_2_Sicherheitsmanagement/Lektion_2_09/Lektion_2_09_node.html. Zugriff am: Jul. 31 2020.

[28] Deutschland, IT-Grundschutz-Methodik: BSI-Standard 200-2, 1. Aufl. Bonn, 2017.

[29] Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz. [Online] Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard203/ITGStandard203_node.html. Zugriff am: Jul. 31 2020.

[30] D. Gilles, Mehr als ein Standardwerk für ein ISMS: Business Continuity Management mit IT-Grundschutz. [Online] Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/Grundschutz/4GS_Tag_2019/Gilles_4GSTag.pdf?__blob=publicationFile&v=3. Zugriff am: Jul. 31 2020.

[31] Bundesamt für Sicherheit in der Informationstechnik, Band B, Kapitel 2: IT-Organisation: Im Umfeld der Hochverfügbarkeit. [Online] Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Hochverfuegbarkeit/BandB/B2_HV-Organisation.pdf?__blob=publicationFile&v=1. Zugriff am: Jul. 31 2020.

[32] Bundesamt für Sicherheit in der Informationstechnik, Übersicht über Branchenspezifische Sicherheitsstandards (B3S). [Online] Verfügbar unter: https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/Was_tun/Stand_der_Technik/B3S/B3S.html?nn=6776460#doc8140926bodyText9. Zugriff am: Jul. 31 2020.

[33] Deutsches Institut für Normung e. V., DIN EN ISO/IEC 27001: Informationssicherheitsmanagementsysteme - Anforderungen (ISO/IEC 27001:2013 + Cor. 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27001:2017. Berlin: Beuth, 2017.

[34] K.-R. Müller, IT-Sicherheit mit System: Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement - Sichere Anwendungen - Standards und Practices, 6. Aufl. Wiesbaden: Springer Fachmedien Wiesbaden, 2018.

[35] Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur europäischen Normung, 2012.

[36] K. Blind, A. Jungmittag und A. Mangelsdorf, Hg., Der gesamtwirtschaftliche Nutzen der Normung: Eine Aktualisierung der DIN-Studie aus dem Jahr 2000, 1. Aufl. Berlin: Beuth, 2011.

[37] Deutsches Institut für Normung e. V., Normung und damit zusammenhängende Tätigkeiten - allgemeine Begriffe (ISOIEC Guide 2:2004): Dreisprachige Fassung EN 45020:2006; mit DIN EN ISO/IEC 17000:2005-03 Ersatz für DIN EN 45020:1998-07 = Standardization and related activities - general vocabulary (ISO/IEC Guide 2:2004), 2007. Aufl. Berlin: Beuth Verlag GmbH, 2007.

[38] Bundesministerium für Wirtschaft und Energie, Normen und Standards. [Online] Verfügbar unter: https://www.bmwi.de/Redaktion/DE/Artikel/Technologie/normen-und-standards.html. Zugriff am: Jul. 31 2020.

[39] Bundesamt für Sicherheit in der Informationstechnik, Zertifizierung von Managementsystemen. [Online] Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Managementsystemzertifizierung/Managementsystemzertifizierung_node.html. Zugriff am: Jul. 31 2020.

[40] H. Kersten, G. Klett und J. Reuter, IT-Sicherheitsmanagement nach der neuen ISO 27001: ISMS, Risiken, Kennziffern, Controls, 2. Aufl., 2020.

[41] Deutsches Institut für Normung e. V., DIN EN ISO/IEC 27000: Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Überblick und Terminologie (ISO/IEC 27000:2018); Deutsche Fassung EN ISO/IEC 27000:2020. Berlin: Beuth Verlag GmbH, 2020.

[42] S. Spörrer, Business Continuity Management: ISO 22301 und weitere Normen im Rahmen der Informationstechnologie. Wiesbaden: Springer Fachmedien Wiesbaden, 2014.

[43] Deutsches Institut für Normung e. V., DIN EN ISO 22300: Sicherheit und Resilienz – Vokabular (ISO 22300:2018); Deutsche Fassung EN ISO 22300:2018. Berlin: Beuth Verlag GmbH, 2018.

[44] Deutsches Institut für Normung e. V., DIN EN ISO 22301: Sicherheit und Resilienz – Business Continuity Management System – Anforderungen (ISO 22301:2019); Deutsche Fassung EN ISO 22301:2019. Berlin: Beuth Verlag GmbH, 2020.

[45] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz): IT-SiG, 2015.

[46] Gesetz zur Kontrolle und Transparenz im Unternehmensbereich: (KonTraG), 1998.

[47] Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz: 2.2 Verantwortung übernehmen. [Online] Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/Webkurs1004/2_NotfallmanagementInitiieren/1_VerantwortungUebernehmen/VerantwortungUebernehmen_node.html. Zugriff am: Jul. 31 2020.

[48] I. Hanschke, Informationssicherheit und Datenschutz systematisch und nachhaltig gestalten: Eine kompakte Einführung in die Praxis, 2. Aufl. Wiesbaden: Springer Fachmedien Wiesbaden GmbH; Springer Vieweg, 2020.

[49] G. Manz, V Vorstand und Aufsichtsrat / 4.1.2.7 Haftungsrisiko Überwachungssystem (§ 91 Abs. 2 AktG), Risikomanagement (Ziff. 4.1.4 DCGK) und Compliance-Management-System (CMS – Ziff. 4.1.4 DCGK). [Online] Verfügbar unter: https://www.haufe.de/recht/deutsches-anwalt-office-premium/v-vorstand-und-aufsichtsrat-4127-haftungsrisiko-ueberwachungssystem-91-abs2-aktg-risikomanagement-ziff414-dcgk-und-compliance-management-system-cms-ziff414-dcgk_idesk_PI17574_HI5560520.html. Zugriff am: Jul. 31 2020.

[50] Wilhelm, Partnerschaft von Rechtsanwälten mbB, Rechtliche Grundlagen der Organhaftung: Pflichten und Haftung des GmbH-Geschäftsführers nach § 43 GmbHG. [Online] Verfügbar unter: https://www.managerhaftungsfall.de/deutsch/grundlagen/. Zugriff am: Jul. 31 2020.

[51] Domscheit und Partner, Partnerschaftsgesellschaft mit beschränkter Berufshaftung, Haftung des Geschäftsführers gegenüber der Gesellschaft. [Online] Verfügbar unter: http://www.domscheit-partner.de/gmbh-geschaeftsfuehrer/haftung-des-geschaeftsfuehrers-gegenueber-der-gesellschaft/. Zugriff am: Jul. 31 2020.

[52] Bundesamt für Sicherheit in der Informationstechnik, Konkretisierung der Anforderungen an die gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen umzusetzenden Maßnahmen: Hinweise zur Umsetzung der Kriterien des § 8a Absatz 1 BSIG für die Beurteilung der Informationssicherheit bei Betreibern Kritischer Infrastrukturen. [Online] Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/Konkretisierung_Anforderungen_Massnahmen_KRITIS.pdf?__blob=publicationFile&v=9. Zugriff am: Jul. 31 2020.

[53] Bundesamt für Sicherheit in der Informationstechnik, Fragen und Antworten zur Regulierung von Anbietern digitaler Dienste - Allgemeine Fragen: Wie definiert das BSI den Begriff Online-Marktplätze? Werden auch Online-Shops von der Regulierung erfasst? [Online] Verfügbar unter: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/DigitaleDienste/FAQ/Allgemein/faq_dsp_allgemein_node.html. Zugriff am: Jul. 31 2020.

[54] S. Meyer, Rechtspflicht zur Compliance? [Online] Verfügbar unter: https://www.bvdcm.de/news/rechtspflicht-zur-compliance. Zugriff am: Jul. 31 2020.

[55] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG: Datenschutz-Grundverordnung. Luxemburg: Amt für amtliche Veröffentlichungen der Europäischen Gemeinschaften, 2018.

[56] Zentralverband des Deutschen Handwerks, Handwerk und Normung: Positionen und Strategie. [Online] Verfügbar unter: https://www.zdh.de/fileadmin/user_upload/Positionspapiere/2020-05-14_ZDH_Positionspapier_-_Handwerk_und_Normung_Freigabe_PRAESIDIUM.pdf. Zugriff am: Jul. 31 2020.

[57] European Committee for Standardization und European Committee for Electrotechnical Standardization, Leitfaden für die Erstellung von Normen unter Berücksichtigung der Bedürfnisse und Belange von Kleinst-, kleinen und mittelständischen Unternehmen (KMU): Deutsche Fassung des CEN/CENELEC-Leitfadens – 17 Guidance for writing standards taking into account micro, small and medium-sized enterprises (SMEs) needs. [Online] Verfügbar unter: ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Guides/17_CENCLCGuide17_DE.pdf. Zugriff am: Jul. 31 2020.

[58] Deutsches Institut für Normung e. V., DIN 820-2: Normungsarbeit – Teil 2: Gestaltung von Dokumenten (ISO/IEC-Direktiven – Teil 2:2018, modifiziert); Deutsche und Englische Fassung CEN/CENELEC-Geschäftsordnung – Teil 3:2019. Berlin: Beuth Verlag GmbH, 2020.

[59] Deutsches Institut für Normung e. V., DIN 1450:2013-04: Schriften - Leserlichkeit. Berlin: Beuth Verlag GmbH.

[60] F. Merges, Assistenzsystem zur Testung und Verbesserung der Lesbarkeit von Gebrauchsinformationen. Siegen, Universität Siegen, Diss., 2014. Siegen: Universitätsbibliothek der Universität Siegen, 2014.

[61] R. Flesch, How to Write Plain English: Chapter 2: Let's Start With the Formula. [Online] Verfügbar unter: https://web.archive.org/web/20160712094308/http://www.mang.canterbury.ac.nz/writing_guide/writing/flesch.shtml. Zugriff am: Jul. 31 2020.

[62] K.-H. Best, „Sind Wort- Satzlänge brauchbare Kriterien zur Bestimmung der Lesbarkeit von Texten?“ in Transferwissenschaften, Bd. 5, Wissenstransfer - Erfolgskontrolle und Rückmeldungen aus der Praxis: [das 5. Kolloquium "Transferwissenschaften" fand in der Zeit vom 29. 9. bis zum 1. 10. 2003 in Göttingen statt], S. Wichter und A. Busch, Hg., Frankfurt am Main: Lang, 2006, S. 21–31.

[63] K. Luttermann und P. Rawinsky, „Fachtexte verstehen in Klarer Sprache“ in Bd. 1, Fach – Sprache – Kommunikation: Fachkommunikation – gelenkt, geregelt, optimiert, F. Heidrich und K. Schubert, Hg., Hildesheim, Hildesheim, Zürich, New York: Universitätsverlag Hildesheim; Georg Olms Verlag, 2020, S. 145–170.

[64] B. M. Bock, U. Fix und D. Lange, Hg., "Leichte Sprache" im Spiegel theoretischer und angewandter Forschung. Berlin: Frank & Timme Verlag für wissenschaftliche Literatur, 2017.

[65] H.-J. Albers, Volkswirtschaftslehre, 6. Aufl. Haan-Gruiten: Verl. Europa-Lehrmittel Nourney Vollmer, 2005.

[66] Deutsches Institut für Normung e. V., Kaufen: Normen und Standards kaufen beim Beuth Verlag - eine DIN-Tochtergesellschaft. [Online] Verfügbar unter: https://www.din.de/de/ueber-normen-und-standards/kaufen. Zugriff am: Jul. 31 2020.

[67] Deutschland <Bundesrepublik> / Bundesverfassungsgericht (BVerfG), Beschluss vom 08.08.1978 - 2 BvL 8/77, 1978.

[68] Deutschland, Handbuch der Rechtsförmlichkeit: Empfehlungen des Bundesministeriums der Justiz für die rechtsförmliche Gestaltung von Gesetzen und Rechtsverordnungen nach § 42 Absatz 4 und § 62 Absatz 2 der gemeinsamen Geschäftsordnung der Bundesministerien, 3. Aufl. Köln: Bundesanzeiger-Verl., 2008.

[69] Bundesamt für Sicherheit in der Informationstechnik, IT-Notfallkarte - Ihr Einstieg ins Notfallmanagement. [Online] Verfügbar unter: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Angebote/IT-Notfallkarte/it-notfallkarte_einstieg_node.html. Zugriff am: Jul. 31 2020.

[70] Arbeitsgemeinschaft Norddeutscher Industrie- und Handelskammern e. V., CORONA-KRISE TRIFFT 92 PROZENT ALLER UNTERNEHMEN IM NORDEN HART: MASSIVE UMSATZRÜCKGÄNGE UND LIQUIDITÄTSPROBLEME. [Online] Verfügbar unter: https://www.ihk-nord.de/blueprint/servlet/resource/blob/4749600/d6a4c43dc2529d4a37a3b1eba4d69dd5/pm-20200330-umfrage-auswirkungen-coronakrise-data.pdf. Zugriff am: Jul. 31 2020.

[71] D. A. J. Sokolov, Coronavirus zwingt Apple zu Gewinnwarnung. [Online] Verfügbar unter: https://heise.de/-4662898. Zugriff am: Jul. 31 2020.

Anlagenverzeichnis

Anlage 1: Merkmale zur Erstellung einer anwenderfreundlichen Norm nach DIN 820, Beiblatt 3:2016-10, Anhang A

A.1 Inhalt einer anwenderfreundlichen Norm

Folgende Sachverhalte dienen der Anwenderfreundlichkeit in Bezug zum Inhalt einer Norm:

— Aufbau und Darstellung einer Norm für betroffene Anwendergruppen verständlich;

— Umfang und Inhalt angemessen;

— zusammenhängende Normen zusammen bearbeitet und aktualisiert;

— genormte Bezeichnungen (Normbezeichnungen) für materielle und immaterielle Gegenstände und Verfahren vorhanden;

— Nenn- und Vorzugsmaße oder Auswahlreihen vorhanden;

— einheitliche Abkürzungen/Kurzzeichen festgelegt und erläutert;

— alle referenzierte Dokumente aufgeführt und öffentlich verfügbar;

— im Vorwort oder in Anhängen alle relevanten Informationen und, wenn nötig, Listung der wichtigsten Änderungen gegenüber der Vorgänger-Ausgabe vorhanden.

A.2 Zusätzliche Aufgaben und Angaben bei der Übernahme von Europäischen und Internationalen Normen

Folgende Punkte verbessern die Anwenderfreundlichkeit einer Norm:

— geklärt, ob Inhalt einer Norm vollständig übernommen oder nationale Restnorm erstellt werden sollte;

— Normbezeichnung für technische Gegenstände und Verfahren vorhanden;

— Sind alle zitierten bzw. mitgeltenden Normen aufgeführt und verfügbar?

— Ersatzvermerke richtig und vollständig.

Anlage 1: Merkmale zur Erstellung einer anwenderfreundlichen Norm nach DIN 820, Beiblatt 3:2016-10, Anhang A [1, S. 11]

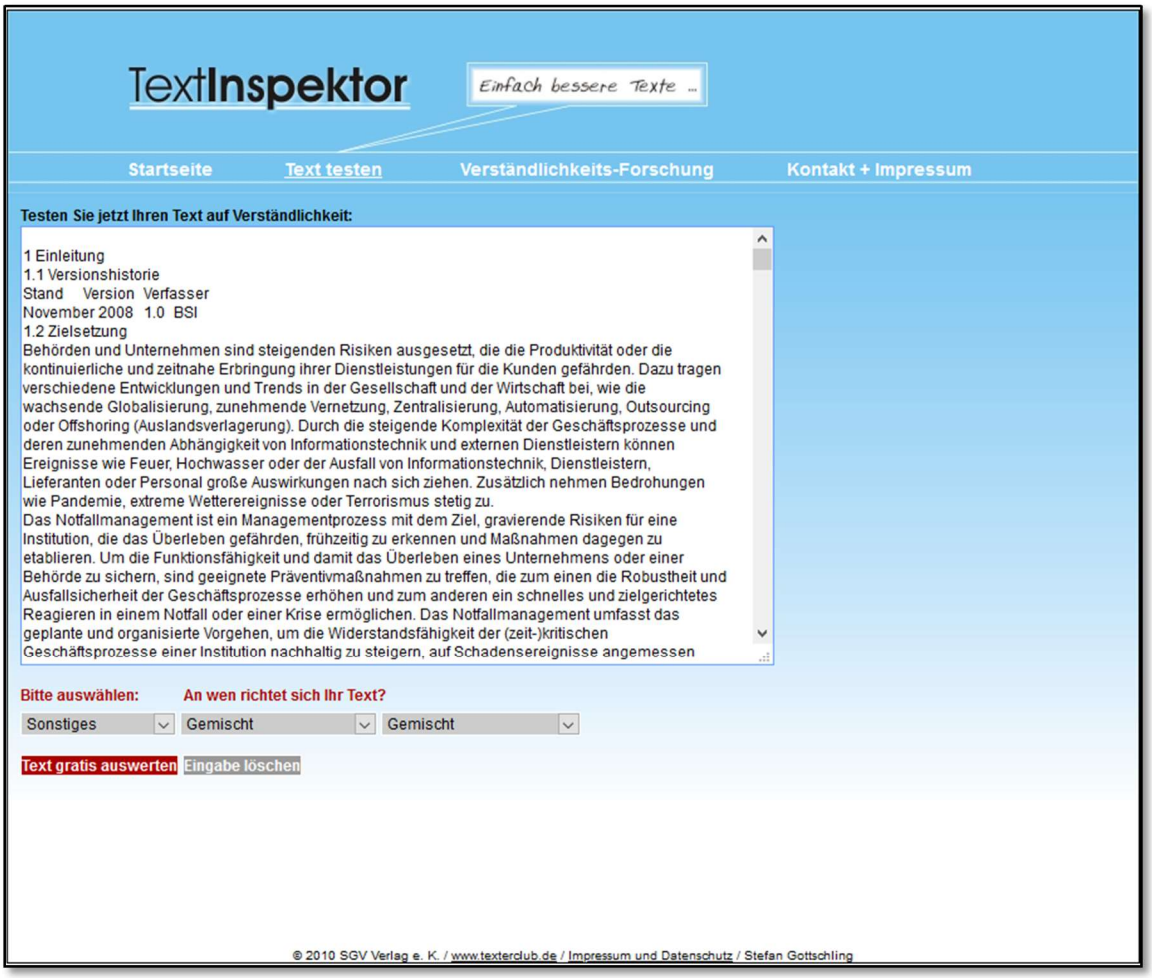
Anlage 2: vollständige Übersicht der Aspekt bezogenen Punktebereiche

Kompatibilitätskriterien	Aspekt	Punktebereich
Vollständigkeit	▪ Alle zum Themenfeld gehöriger Normen, inklusive Querschnittsnormen sind aufgelistet ▪ Die im Anwendungsbereich genannten Inhalte sind vollständig	▪ n. a. ▪ 0, 4
Aufbau	▪ Erstellungsmotivation ▪ Benennung Normenziel sowie Zielgruppe ▪ gute Übersichtlichkeit ▪ relevante Informationen schnell auffindbar ▪ nachvollziehbare Versionsänderungen	▪ 0, 4 ▪ 0, 2, 4 ▪ n. a. ▪ 1 bis 4 ▪ 0, 4
Lesbarkeit und Verständlichkeit	▪ leichte Lesbarkeit ▪ allgemeinverständliche Sprache ▪ Abkürzungen sind erklärt ▪ komplizierte Ausdrücke sind erklärt und ggf. in einem Kapitel „Begriffe“ aufgenommen ▪ Vermittlung von Grundlagenwissen ▪ Nutzung von Beispielen, weiteren Erklärungen oder Veranschaulichungen ▪ Normenlänge so kurz wie nötig ▪ Vermeidung von Querverweisen innerhalb der Normen ▪ Vermeidung von Verweisungen auf andere Normen, ggf. Text zitieren ▪ deutsche Sprache ▪ Vermeidung inhaltlicher und thematischer Norm-Dopplungen	▪ 1 bis 4 ▪ n. a. ▪ 0, 4 ▪ n. a. ▪ n. a. ▪ 1 bis 4 ▪ n. a. ▪ 1 bis 4 ▪ 1 bis 4 ▪ 0, 4 ▪ n. a.

Kompatibilitätskriterien	Aspekt	Punktebereich
Wirtschaftlichkeit	▪ Normen-Zugänglichkeit ▪ Verhältnismäßigkeit der entstehenden Kosten durch Normeinführung ▪ Normen spiegeln den am Markt verfügbaren Stand der Technik wider ▪ vereinfachte Rechenverfahren verwenden	▪ 0, 4 ▪ 1 bis 4 ▪ n. a. ▪ 0, 4
Prüfbarkeit der Anforderungen	▪ Definierter Anwendungsbereich ▪ Anforderungen als Leistungsmerkmale ausgedrückt	▪ 0, 4 ▪ 0, 4

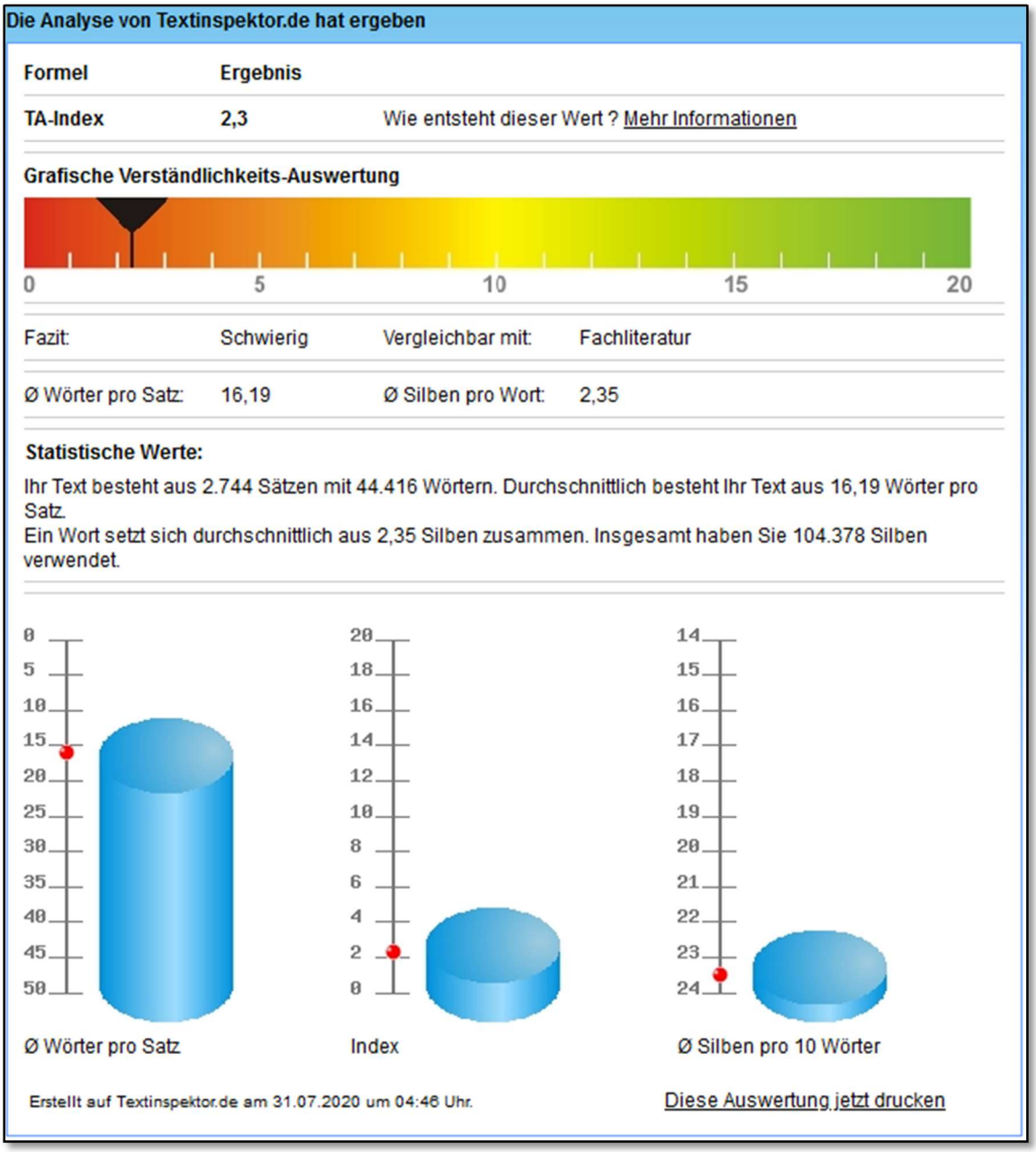
Anlage 2: vollständige Übersicht der Aspekt bezogenen Punktebereiche

Anlage 3: Auszug der Bestimmung der statistischen Textauswertung des BSI-Standards 100-4



Anlage 3: Texteingabe des BSI-Standards 100-4 in der Webseite http://textinspektor.de/text_testen.php5 zur Bestimmung statistischer Werte

Anlage 4: Auszug von dem Ergebnis der statistischen Textauswertung des BSI-Standards 100-4



Anlage 4: Ergebnis der Textanalyse des BSI-Standards 100-4 über die Webseite http://textinspektor.de/text_testen.php5

Eigenständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe. Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Berlin, 31.07.2020 Mark Le Corre