Jade Hochschule
Wilhelmshaven/ Oldenburg/ Elsfleth

Fachbereich Management, Information, Technologie
Labor für Datenkommunikation
und Netzwerktechnik

Bachelorarbeit

zur Erlangung des akademischen Grades
Bachelor of Science

Anwendung von Informationssicherheitsstandards zur Erfüllung rechtlicher Anforderungen

Utilization of Information Security Standards to meet legal Requirements

Erstgutachter: Prof. Dr. rer. nat. Matthias Berger

Zweitgutachter: Dipl. Wirtschaftsinf. Sascha Fankhänel

Wilhelmshaven, 09. Juli 2024

Selbstständigkeiteserklärung

Hiermit erkläre ich, dass ich meine Bachelorarbeit mit dem Titel „Anwendung von Informationssicherheitsstandards zur Erfüllung rechtlicher Anforderungen“ selbstständig und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe und dass ich alle Stellen, die ich wörtlich oder sinngemäß aus Veröffentlichungen entnommen habe, als solche kenntlich gemacht habe. Die Arbeit hat bisher in gleicher oder ähnlicher Form oder auszugsweise noch keiner Prüfungsbehörde vorgelegen.

Wilhelmshaven, 09. Juli 2024 [redacted]

Ort, Datum

Kurzfassung

Mit fortschreitender Digitalisierung stehen sowohl staatliche Institutionen als auch Unternehmen einen erhöhtem Bedrohungspotential gegenüber. Um dieser Bedrohung adäquat zu begegnen, hat die Europäische Union, im Jahr 2019, die Sicherheitsunion 2020-2025 beschlossen. Aus dieser Sicherheitsunion entspringen unter Anderem Gesetze und Richtlinien, welche sich mit der digitalen Resilienz beschäftigen und bei Umsetzung zu einer erhöhten Resilienz führen sollen. Bei der Umsetzung der Gesetze und ihren Anforderungen stehen primär Klein- und mittelständische Unternehmen (KMU) vor einer großen Hürde. Hier fehlt oft Expertise und Personal, um sich adäquat mit den Anforderungen und möglichen Maßnahmen auseinanderzusetzen.

Ziel dieser Arbeit ist es einen Katalog zu erstellen, welcher Anforderungen aus den relevanten Gesetzen mit Maßnahmen aus etablierten Informationssicherheitsstandard in Relation bringt. Hierzu werden die folgenden zugrundeliegenden Fragestellungen beantwortet: Welche relevanten gesetzlichen Änderungen bringt die Sicherheitsunion 2020-2025 hervor? Welche Maßnahmen, aus etablierten Standards, können zu einer Konformität mit den jeweiligen gesetzlichen Anforderungen führen?

Zur Beantwortung dieser Fragestellungen wurde im ersten Schritt eine Analyse der relevanten Gesetze vorgenommen und die daraus resultierenden Anforderungen in einem Katalog festgehalten. Anschließend erfolgte eine Analyse relevanter Informationssicherheitsstandards, um geeignete Maßnahmen zur Erfüllung der Anforderungen zu identifizieren. Im letzten Schritt wurde ein handlicher Katalog erstellt, welcher die gesetzlichen Anforderungen mit den identifizierten Maßnahmen in Relation setzt.

Der entstandene Katalog zeigt, dass die ausgewählten Standards und Normen eine gute Basis für die Konformität mit den gesetzlichen Anforderungen darstellen. Es konnten für die 76 identifizierten gesetzlichen Anforderungen, welche relevant für KMU sind, 540 Anforderungs- und Maßnahmenpaare gebildet werden. Auch bei dieser Anzahl der gebildeten Paaren, kann keiner der aufgeführten Standards bzw keine Norm eine vollumfängliche Konformität mit allen identifizierten Gesetzen bzw Verordnungen gewährleisten. Dies ist primär auf die jeweiligen Anwendungsbereiche und Zielführungen der Werke zurückzuführen ist.

Weiterführende Arbeiten könnten sich mit der qualitativen Überprüfung und Beurteilung der gebildeten Anforderungs- und Maßnahmenpaaren beschäftigen. Darüber hinaus erscheint es sinnvoll, die Effektivität der verschiedenen Informationssicherheitsstandards in unterschiedlichen branchenspezifischen Kontexten zu analysieren und zu vergleichen, um zu dem jeweiligen Kontext den effektivsten Standard zu wählen.

Abstract

As digitalization progresses, both state institutions and companies are facing an increased threat potential. In order to adequately counter this threat, the European Union adopted the Security Union 2020-2025 in 2019. Among other things, this Security Union gives rise to laws and guidelines that deal with digital resilience and are intended to lead to increased resilience when implemented. When it comes to implementing the laws and their requirements, small and medium enterprises in particular face a major hurdle. They often lack the expertise and personnel to adequately deal with the requirements and possible measures.

The aim of this work is to create a catalog that compares requirements from the relevant laws with measures from established information security standards. The following underlying questions are posed: What relevant legal changes will the Security Union 2020-2025 bring about? Which measures from established standards can lead to conformity with the respective legal requirements?

To answer these questions, the first step was to analyze the relevant laws and record the resulting requirements in a catalog. This was followed by an analysis of relevant information security standards in order to identify suitable measures to fulfill the requirements. In the final step, a manageable catalog was created that compares the legal requirements with the identified measures.

The resulting catalog shows that the selected standards and norms represent a good basis for conformity with the legal requirements. 76 pairs of requirements and measures could be formed for the 103 identified legal requirements that are relevant for KMU. Even with this number of pairs formed, none of the listed standards or norms can guarantee full conformity with all identified laws or regulations. This is primarily due to the respective areas of application and objectives of the plants.

Further work could deal with the qualitative review and assessment of the pairs of requirements and measures formed. In addition, it seems sensible to analyze and compare the effectiveness of the various information security standards in different industry-specific contexts in order to select the most effective standard for the respective context.

Inhaltsverzeichnis

Abkürzungsverzeichnis

BBK Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

BCM Business Continuity Management

BIA Business Impact Analyse

BIDT Bayerisches Forschungsinstitut für Digitale Transformation

BSI Bundesamt für Sicherheit in der Informationstechnik

BYOD Bring-Your-Own-Device

C5 Cloud Computer Compliance Criteria Catalogue

CER Critical Entities Resilience

CRA Cyber Resilience Act

DGSVO EU-Datenschutzgrundverordnung

DORA Digital Operational Resilience Act

EBA European Banking Authority

EIOPA European Insurance and Occupational Pensions Authority

ENISA European Union Agency for Cybersecurity

ESA European Supervisory Authorities

ESMA European Securities and Markets Authority

KMU Kleine und mittlere Unternehmen

IEC International Electrotechnical Commission

IKT Informations- und Kommunikationstechnik

ISMS Informationssicherheitsmanagementsystemen

ISO Internationale Orgranisation für Normung

KMU Klein- und mittelständische Unternehmen

RTS Regulatory Technical Standards

TLPT Threat-Lead-Penetration-Testing

Gender Hinweis

Zur besseren Lesbarkeit wird in der vorliegenden Arbeit das generische Maskulinum verwendet. Die in dieser Arbeit verwendeten Personenbezeichnungen beziehen sich - sofern nicht anderweitig kenntlich gemacht - auf alle Geschlechter.

1 Einleitung

Das nachfolgende Kapitel stellt den Einstieg in die vorliegende Arbeit dar. Zu Beginn wird die Motivation erläutert, welche zu der Auswahl des Themas geführt hat. Im Anschluss werden die daraus resultierenden Fragestellungen thematisiert. Hierbei wird konkret auf die Fragestellungen eingegangen und wie diese, im Verlauf der Arbeit, beantwortet werden. Der letzte Abschnitt des Kapitels dient dazu, dem Leser einen Überblick über die Arbeit im Ganzen zu bieten. Hierbei wird auf jedes der nachfolgenden Kapitel eingegangen.

1.1 Motivation

Die Digitalisierung nimmt in Unternehmen, Behörden und bei den Verbrauchern immer weiter zu. Dies ist unter anderem auf die Covid-19 Krise zurückzuführen. Der stetige Ausbau der Digitalisierung bietet jedoch zugleich eine breite Angriffsfläche für Akteure. Verizon veröffentlicht jährlich einen Data Breach Report, welcher Trends in der Informationssicherheit und Angriffsmustern aufzeigt. Im Jahr 2020 konnte Verizon hierbei 3950 bestätigte Breaches verbuchen, während es im Jahr 2024 bereits 10626 Breaches gewesen sind (vgl. [VER20], S.6; [VER24], S.5). Auf nationaler Ebene verdeutlicht der IT-Sicherheitslagebericht, des Bundesamts für Sicherheit in der Informationstechnik (BSI), die akute Bedrohungslage. Dieser verbucht täglich einen Zuwachs von rund 250.000 Schadprogrammvarianten (vgl. [BUN24a], S.6). Im Falle eines Sicherheitsvorfalls kann erheblicher Schaden auf betroffene Unternehmen zukommen. Bitkom gibt hierbei in einer Studie an, dass der Gesamtschaden bei rund 206 Milliarden Euro im Jahr 2023 liegt, welcher auf Datendiebstahl, Industriespionage oder Sabotage zurückzuführen ist[1].
Im Vordergrund der Angriffe stehen hierbei oft KMU, da diese 99,4 Prozent der Wirtschaftsunternehmen in Deutschland ausmachen (vgl. [BUN24a], S.64). Die Attraktivität dieser Unternehmen für Angriffe ist weitgehend auf zwei übergeordnete Punkte zurückzuführen. Zum einen sind diese oft innovativ und zum anderen können diese in die Lieferketten von Großunternehmen eingebunden sein, was sie zu einem idealen ersten Ziel macht (vgl. [RIT18], S. 231).

Um diesem ansteigenden Trend entgegenzuwirken, hat die Europäische Union die Sicherheitsunion 2020-2025 beschlossen (vgl. [EUR20]). Ein Pfeiler dieser Sicherheitsunion ist ein zukunftstaugliches Sicherheitsumfeld und beschäftigt sich unter anderem mit der Cybersicherheit[2]. In diesem Rahmen wurden bereits und werden weiterhin EU-weite Gesetze und Verordnungen verabschiedet. Anzuführende Beispiele für solche Gesetze bzw. Verordnungen sind: der „Cyber Resilience Act“, die „The

[1] EV, Bitkom (2024): Organisierte Kriminalität greift verstärkt die deutsche Wirtschaft an, in: Bitkom, 02.02.2024, unter: https://www.bitkom.org/Presse/Presseinformation/Organisierte-Kriminalitaet-greift-verstaerkt-deutsche-Wirtschaft-an [Zugriff: 21.05.2024]

[2] Europäische Sicherheitsunion (2020): Europäische Kommission, unter: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/european-security-union$_{e}$n[Zugriff: 21.05.2024]

Network and Information Security Directive“ in der zweiten Version oder auch der „Digital Operational Resilience Act“.

Mit diesen Gesetzen bzw. Richtlinien geht simultan eine Umsetzungsverpflichtung, für die Mitgliedsstaaten, einher. Diese nationale Umsetzung kann jedoch gerade für KMU schwierig werden, da diese oft nicht über dedizierte Informationssicherheitsteams verfügen. In solchen Unternehmen fehlt es folglich an Expertise und bereitgestellten finanziellen Mitteln, um eine Konformität mit den aktuellen komplexen Änderungen zu erreichen. Bei der Findung von konkreten Maßnahmen, zur Konformität, gibt es eine Vielzahl von Einflussfaktoren, welche zu beachten sind. So muss ein Online-Handelsplatz zusätzliche Gesetze beachten, welche beispielsweise die Datenverarbeitung betreffen (vgl. 2.1.5).
Oft leisten die verabschiedeten Gesetze hier keine Abhilfe. Es werden verpflichtende Mindestmaßnahmen festgelegt, jedoch gilt es für jedes Unternehmen selbst zu evaluieren, welche Maßnahmen ergriffen werden, da oft eine Konkretisierung der Maßnahmen im Gesetz stattfindet. Vor dem Hintergrund der fehlenden Expertise stehen die betroffenen Unternehmen vor einem schwer zu lösendem Problem.

1.2 Zielsetzung

Um die zuvor erwähnte Problematik zu adressieren, zielt die vorliegende Arbeit darauf ab, einen handlichen Anforderungs- und Maßnahmenkatalog zu erarbeiten. Zugrunde hierfür liegen folgende Fragestellungen: Welche relevanten gesetzlichen Änderungen treten von 2020 bis 2025 in Kraft und welche Anforderung an die Informationssicherheit stellen diese? Welche Maßnahmen, aus etablierten Normen und Standards, können zur Konformität sorgen?

Der resultierende Anforderungs- und Maßnahmenkatalog soll zur besseren Übersicht anhand der Gesetze gruppiert werden. Um den Anforderungs- und Maßnahmenkatalog als Ziel zu erreichen, werden in dem Grundlagenteil die relevanten Gesetze und Richtlinien analysiert und die jeweils geforderten Anforderungen erfasst. Im weiteren Verlauf des Kapitels werden etablierte Standards und Normen herangezogen und ein Überblick über diese gegeben. Im Praxisteil der Arbeit werden den gesetzlichen Anforderungen die jeweils passenden Maßnahmen zugewiesen.

1.3 Kapitelübersicht

Das erste Kapitel der vorliegenden Arbeit dient, neben der Übersicht, dem Zweck den Leser in das Thema und die Vorgehensweise einzuleiten. Im Anschluss wird in Kapitel zwei auf den gesetzlichen Rahmen eingegangen. Hierzu werden zunächst die relevanten europäischen Regelungen herangezogen und im Anschluss die nationalen deutschen Regelungen. Ziel dieses Kapitels ist es, eine theoretische Grundlage zu bieten und am Ende des Kapitels den erwarteten Anforderungskatalog zu erarbeiten.

Das dritte Kapitel widmet sich den etablierten Normen und Standards. Innerhalb der Unterkapitel wird immer auf einen Standard eingegangen, je ein Überblick gegeben und die jeweils relevanten Maßnahmen aus den Normen/Standards herausgefiltert. Sind sowohl die Anforderungen, als auch die Maßnahmen erfasst, werden diese im vierten Kapitel in Korrelation gebracht. Dieses Kapitel stellt den Hauptarbeitsteil der vorliegenden Arbeit dar und dient dem Zweck der Erläuterung, der einzelnen Überlegungen. Im Anschluss wird im fünften Kapitel der erarbeitete Katalog einer Betrachtung unterzogen, welche eine kritische Beleuchtung des erarbeiteten Ergebnisses darstellt. Zuletzt erfolgt im sechsten Kapitel eine Zusammenfassung der Ergebnisse, die konkrete Beantwortung der Fragestellung und ein Ausblick, welcher über die zukünftigen Schritte aufklärt.

2 Gesetzliche Rahmenbedingungen

Das nachfolgende Kapitel stellt einen Überblick über die, in dem Betrachtungszeitraum anfallenden, Regulierungen dar. Hierbei wird zunächst auf europäische Regulierungen eingegangen, wobei stets eine Analyse erfolgt und im Anschluss die, aus der Regulierung hervorgehenden, Anforderungen thematisiert werden. Im Anschluss an die europäischen Regulierungen erfolgt anhand von dem selbigen Vorgehen eine Analyse von nationalen Regulierungen.

2.1 Europäische Regulierungen

In dem betrachteten Zeitraum fallen eine Vielzahl von Verordnungen und Richtlinien auf europäischer Ebene an. Nachfolgend werden die von dem Autor als am relevantesten betrachteten Regulierungen thematisiert.

2.1.1 Cyber Resilience Act

Der Vorschlag für eine Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen, auch bekannt als der „Cyber Resilience Act“, wurde der Europäischen Kommission, am 15. September 2022, vorgelegt (vgl. [EURb]). Der Vorschlag wurde noch nicht durch eine Verordnung finalisiert und befindet sich zum aktuellen Zeitpunkt in Diskussion, durch den Europäischen Rat [1]. Voraussichtlich soll die Verordnung 2024 in Kraft treten. [2]

Hintergrund für die Verordnung ist die Entwicklung der Cyberangriffe der letzten Jahre (vgl. [EURb], Begründung 1., *Gründe und Ziele des Vorschlags*). Hierbei sind alleine in Deutschland vom 1. Juni 2022 bis zum 30. Juni 2023 insgesamt rund 27.000 neue Schwachstellen in Softwareprodukten bekannt geworden. Dies stellt eine Steigerung von rund 24 Prozent im Vergleich zum Vorjahr dar (vgl. [BUN24a], S. 33). Auch im Bereich der Hardwareprodukte sind weitere Schwachstellen bekannt geworden. So ist im März 2023 eine Zero-Day-Schwachstelle bekannt geworden, welche in Verbindung mit Exynos-Modemchips funktionsfähig ist (vgl. [BUN24a], S. 39). Betroffen von dieser Schwachstelle sind eine Reihe von Samsung Smartphones, Vivo Smartphones, Google Pixel 6 und 7 Geräte und Fahrzeuge, welche den „Exnos Auto T5123 Chip“ verwenden [3].

Inhaltlich fokussiert die Verordnung den Bereich der Produkte mit digitalen Elementen, was Software-

[1] EUR-LEX - 2022_272 - EN - EUR-LEX. http://eur-lex.europa.eu/procedure/EN/2022$_2$72 [Zugriff: 28.06.2024]

[2] EU Cyber Resilience Act. (n.d.). Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act [Zugriff: 28.06.2024]

[3] Zero, G. P. (n.d.). Multiple internet to baseband remote code execution vulnerabilities in Exynos modems. https://googleprojectzero.blogspot.com/2023/03/multiple-internet-to-baseband-remote-rce.html [Zugriff: 28.06.2024]

oder Hardwarekomponenten mit Datenfernverarbeitungslösungen beinhaltet (vgl. [EURb], Art. 3 (1)). Hierzu wird Wirtschaftsakteuren (Hersteller, Einführer und Händler) eine Reihe von Pflichten auferlegt. Die Verordnung sieht vor, die Produkte mit digitalen Elementen in unterschiedliche Kritikalitätsstufen aufzuteilen, welche die Anforderungen an Produkte, und damit auch die Anforderungen an Wirtschaftsakteure, je nach Stufe verschärfen (vgl. [EURb], Anhang 3).

Auf Herstellerseite sieht der Gesetzesentwurf vor, dass über den gesamten Produktlebenszyklus Sicherheitslücken, durch angemessene Maßnahmen, zu schließen sind (vgl. [EURb], Art. 10). Ebenfalls wird eine doppelte Meldepflicht für Hersteller eingeführt. Konkret bedeutet dies, dass bei Kenntnisnahme einer ausgenutzten Schwachstelle, innerhalb von 24 Stunden die ENISA informieren. Weiterhin sind die Empfänger des betroffenen Produktes über die Schwachstelle und Korrekturmaßnahmen, falls bereits vorhanden, zu informieren (vgl. [EURb], Art. 11).

Personen, welche Produkte mit digitalen Elementen einführen müssen sicherstellen, dass diese den Anforderungen, an die geltende Kritikalitätsstufe, genügen. Weiterhin ist sicherzustellen, dass diese den Konformitätsanforderung an das Produkt selber (Herstelleranforderungen) gewährleisten. Sollte ein Einführer den Verdacht haben, dass ein Produkt mit digitalen Elementen nicht den Anforderungen entspricht, hat er die zuständige Aufsichtsbehörde zu informieren und Korrekturmaßnahmen, welche zur Konformität führen, auszuführen (vgl. [EURb], Art. 13).

Händler von Produkten mit digitalen Elementen sind nach dieser Verordnung dazu verpflichtet sicherzustellen, dass die Produkte den nötigen Anforderungen entsprechen und ebenfalls ein CE-Kennzeichen auf dem Produkt vorhanden ist. Sollte der Händler davon ausgehen, dass ein, in dieser Verordnung angesprochenes Produkt, ein Cybersicherheitsrisiko darstellt, hat dieser unverzüglich nach Kenntnisnahme die nationale Marktaufsichtsbehörde zu unterrichten und Korrekturmaßnahmen vorzunehmen (vgl. [EURb], Art. 14).

Diese Regulierung wurde für die vorliegende Arbeit ausgewählt, da sie einen essenziellen Beitrag zu der allgemeinen Informationssicherheit leistet. Durch die gesetzlichen Anforderungen an die Produkte selber, ist für den Endverbraucher sichergestellt, dass die auf dem Markt vorhandenen Produkte über ausreichende Sicherheitsvorkehrungen verfügen. Die Verordnung verpflichtet hierzu die gesamte Lieferkette, was zwar zu einem erhöhten Aufwand bei Wirtschaftsakteuren sorgt, jedoch können diese durch die Regulierungen ebenfalls einfacher in den Markt weiterer Mitgliedsstaaten eindringen, da es vereinheitlichte Anforderungen gibt.

2.1.2 Digital Operational Resilience Act

Der „Digital Operational Resilience Act (DORA)“[EUR23d], wurde am 14. Dezember 2022 durch das Europäische Parlament und Rat veröffentlicht und findet ab dem 17. Januar 2025 Anwendung (vgl. [EUR23d], Art. 64).

Seit Jahren findet in allen Bereichen des täglichen Lebens eine Transformation, aufgrund der fortschreitenden Digitalisierung, statt. Diese digitale Transformation treibt auch den Einsatz von IKT-Systemen im Finanzsektor voran, was jedoch mit einem erhöhten IKT-Risiko einhergeht (vgl.[EUR23d], Beweggrund (1)). Diesen Umstand hat das Europäische Parlament und Rat, nebst 105 weiteren Beweggründen, welche sich im Kern zu meist mit IKT-Risiken beschäftigen, zum Anlass genommen und DORA verabschiedet. Mit der Implementierung von DORA verfolgt die Europäische Union das Ziel, ein „hohes gemeinsames Niveau an digitaler operationaler Resilienz“([EUR23d], Art. 1), im Finanzsektor, zu erreichen.

Geltungsbereich	
„Finanzunternehmen“	Kreditinstitute, Zahlungsinstitute, Kontoinformationsdienstleister, E-Geld-Institute, Wertpapierfirmen, Krypto-Dienstleistungsanbieter, Zentralverwahrer, zentrale Gegenparteien, Handelsplätze, Transaktionsregister, Verwalter alternativer Investmentfonds, Verwaltungsgesellschaften, Datenbereitstellungsdienste, Versicherungs- und Rückversicherungsunternehmen, Versicherungsvermittler, Einrichtungen der betrieblichen Altersversorgung, Ratingagenturen, Administratoren kritischer Referenzwerte, Schwarmfinanzierungsdienstleister, Verbriefungsregister, IKT-Drittdienstleister
Ausgeschlossen	Verwalter alternativer Investmentfonds nach Art. 3 Abs.2 Richtlinie 2011/61/EU; Versicherungs- und Rückversicherungsunternehmen nach Art. 4 2009/138/EG; Einrichtungen der betrieblichen Altersversorgung mit weniger als 15 Versorgungsanwärtern, natürliche und juristische Personen nach Art.2&3 2014/65/EU, Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit, bei denen es sich um Kleinstunternehmen oder kleine oder mittlere Unternehmen handelt; Postgiroämter im Sinne von Artikel 2 Absatz 5 Nummer 3 der Richtlinie 2013/36/EU

Tabelle 2.1: DORA: Geltungsbereich
(nach [EUR23d], Art. 2)

Tabelle 2.1 zeigt den Geltungsbereich von DORA. Wie zu erkennen ist, ist dieser beinahe allumfassend, bezüglich den im Finanzsektor ansässigen Unternehmenssparten und schließt lediglich spezifische Fälle aus, welche bereits durch andere Regulierungen geregelt sind.

Da DORA ein hohes Maß an digitaler Resilienz anstrebt, besteht der Regelungsinhalt aus mehreren Bereichen, welche gemeinsam einen umfassenden Schutz bieten sollen:

IKT-Risikomanagement (Art. 5-16): DORA fordert von den betroffenen Unternehmen die Implementierung eines IKT-Risikomanagementrahmen (vgl. [EUR23d], Art. 6). Der Rahmen soll den Unternehmen dabei helfen ihre Funktionsfähigkeit aufrechtzuerhalten. Elementare Bausteine sind dabei Maßnahmen zur Identifizierung (vgl. [EUR23d], Art. 8), Schutz und Prävention (vgl. [EUR23d], Art. 9), Erkennung (vgl. [EUR23d], Art. 10), Reaktion und Wiederherstellung (vgl. [EUR23d], Art. 11), Lernprozesse und Weiterentwicklung (vgl. [EUR23d], Art. 13) und Kommunikation (vgl. [EUR23d], Art. 14). Spezifizierende Anforderungen sind durch den Gesetzgeber, gemäß Artikel 15, in einem technischen Regelungsstandard entworfen worden [EURa].

Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle (Art. 17-23): Weiterhin fordert DORA die Implementierung eines Managementprozesses, welcher die Überwachung, Protokollierung und Meldung von IKT-bezogenen Vorfällen behandelt (vgl.[EUR23d], Art. 17). Die Klassifizierung der IKT-Vorfälle wird hierbei nach einem Schema stattfinden, welches von den drei European Supervisory Authorities (ESA) (European Banking Authority (EBA), European Insurance and Occupational Pensions Authority (EIOPA), European Securities and Markets Authority (ESMA)) in Kooperation mit der European Union Agency for Cybersecurity (ENISA) entworfen wurde (vgl. [EUR24b]). Sollte ein aufgetretener IKT-Vorfall als schwer klassifiziert worden sein, so ist dieser durch das Unternehmen an die nationale Aufsichtsbehörde zu melden (vgl. [EUR23d], Art. 19 (1)). Weiterhin bietet DORA Finanzunternehmen die Möglichkeit, erhebliche Cyberbedrohungen freiwillig zu melden (vgl.[EUR23d], Art. 19 (2)).

Testen der digitalen operationalen Resilienz (Art. 24-27): In Vorbereitung auf ggf. eintretende IKT-Vorfälle fordert DORA ein Testen der digitalen operationalen Resilienz. Damit einhergehend sind Finanzunternehmen verpflichtet, ein Programm zu entwerfen, nachdem die IKT-Tools und Systeme getestet werden (vgl.[EUR23d], Art. 24). Diese Tests können für ausgewählte Finanzunternehmen in Form eines Threat-Lead-Penetration-Testing (TLPT) gefordert sein (vgl.[EUR23d], Art. 26 (8)).

Management des IKT-Drittrisikos (Art. 28-30): Zur Adressierung von Risiken bei der Nutzung von IKT-Dienstleistungen mit Drittdienstleistern fordert DORA bei Vertragsabschluss eine Risikoanalyse und Due-Diligence (vgl.[EUR23d], Art.28).

Überwachungsrahmen für kritische IKT-Drittdienstleister (Art. 31-44): Dieser Abschnitt der Verordnung regelt die Schaffung eines harmonisierten Überwachungsrahmens. Dieser bezieht sich weniger auf Anforderungen an Unternehmen, sondern beschreibt die Aufgaben und Befugnisse der Stellen, welche die Unternehmen überwachen. Aus diesem Grund ergehen aus diesem Abschnitt der Verordnung nur wenige indirekte Anforderungen bzw. Pflichten an der IKT-Dienstleister. Konkret

muss der IKT-Dienstleister, nach Anforderung, Informationen bereitstellen, damit die Aufsichtsbehörde ihrer Pflicht nachgehen kann (vgl. [EUR23d], Art. 37). Zudem können Inspektionen durch die Aufsichtsbehörde erfolgen (vgl. [EUR23d], Art. 39). Weiterhin kann die Aufsichtsbehörde kann Empfehlungen an die IKT-Dienstleister richten. Der IKT-Dienstleister ist im Anschluss, innerhalb von 60 Kalendertagen, dazu verpflichtet, der Aufsichtsbehörde die Unternehmensabsicht zu der Empfehlung mitzuteilen (vgl. [EUR23d], Art. 42 (1)).

Vereinbarung über den Austausch von Informationen (Art.45): DORA erkennt die Wichtigkeit von Zusammenarbeit zwischen den IKT-Dienstleistern an und möchte dementsprechend einen Rahmen zum Austausch von Informationen schaffen. Ein solches Kollaborationsumfeld soll die Ausbreitung von IKT-bezogenen Sicherheitsvorfällen eingrenzen und zeitgleich die Widerstandsfähigkeit, durch Informationsaustausch, stärken (vgl. [EUR23d], Art.45). Hierbei ist wichtig zu erwähnen, dass diese Zusammenarbeit auf Freiwilligkeit beruht und keine Verpflichtung hierzu aus DORA ergeht.

Der Gesetzgeber will zum Zweck der Konformität eine Reihe von *Regulatory Technical Standards (RTS)* verabschiedet, welche Mindestanforderungen beschreiben. Zum Zeitpunkt des Verfassens wurden bereits folgende RTS veröffentlicht, welche ergänzende Spezifikationen festlegen:

1. RTS über den Risikomanagementrahmen ([EUR24d]
2. RTS über die Klassifizierung von IKT-Vorfällen ([EUR24b])
3. RTS Leitlinie für vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden ([EUR24c])

Die daraus ergehenden Anforderungen werden im weiteren Verlauf jedoch nicht einbezogen, da dies zu Umfangreich für die vorliegende Arbeit wäre. Die im weiteren Verlauf beachteten Anforderungen sind Anhang A.1 zu entnehmen.

2.1.3 Critical Entities Resilience Directive

Die Richtlinie (EU) 2022/2557, auch bekannt als „Critical Entities Resilience Directive“ (CER), ist am 14. Dezember 2022 vom Europäischen Parlament verabschiedet worden (vgl. [EUR23b]). Ziel dieser Verordnung besteht darin, die physische Resilienz von kritischen Infrastrukturen innerhalb der Europäischen Union zu regulieren (vgl. [EUR23b], Art. 1).

Der Anwendungsbereich, der CER-Richtlinie, beschränkt sich auf Unternehmen, welche „Essential Services“ in spezifischen Sektoren erbringen. Dieser Anwendungsbereich ist im Vergleich zu der abgelösten Verordnung deutlich ausgeweitet. Tabelle 2.2 zeigt eine Gegenüberstellung beider Anwendungsbereiche.

2008/113/EG	CER
1. Energie a) Strom b) Öl c) Gas 2. Verkehr a) Straßenverkehr b) Schienenverkehr c) Luftverkehr d) Binnenschifffahrt e) Hochsee- und Küstenschifffahrt und Häfen	1. Energie a) Strom b) Fernwärme und -kälte c) Erdöl d) Erdgas e) Wasserstoff 2. Verkehr a) Luftfahrt b) Schienenverkehr c) Schifffahrt d) Straßenverkehr e) Öffentlicher Verkehr 3. Bankwesen 4. Finanzmarktinfrastruktur 5. Gesundheit 6. Trinkwasser 7. Abwasser 8. Digitale Infrastruktur 9. Öffentliche Verwaltung 10. Weltraum 11. Produktion, Verarbeitung und Vertrieb von Lebensmitteln

Tabelle 2.2: Vergleich: Anwendungsbereich 2008/113/EG und CER

Für die Mitgliedsstaaten besteht eine Verpflichtung, bis zum 17. Juli 2026, die bei ihnen anfallenden nationalen kritischen Infrastrukturen zu ermitteln (vgl. [EUR23b], Art. 7 Satz 1).

Sobald die Mitteilung über Einstufung als „Critical Entity“ eingegangen ist, hat die betroffene

Einrichtung eine Risikobewertung vorzunehmen, welche darauf abzielt Ausfallrisiken zu identifizieren und bewerten (vgl. [EUR23b], Art. 12). Die betroffenen Einrichtungen sind im Weiteren durch die Verordnung dazu verpflichtet, eine Reihe von Maßnahmen zu treffen, welche das Ziel haben die physische Resilienz der Einrichtung zu erhöhen. Konkret werden hier *„verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen“* gefordert (vgl. [EUR23b], Art. 13)). Diese Maßnahmen sollen das Auftreten von Sicherheitsvorfällen vermeiden, einen angemessenen physischen Schutz der kritischen Infrastruktur und Räumlichkeiten gewährleisten, auf einen auftretenden Vorfall reagieren und Schadenbegrenzung gewährleisten, dabei helfen, im Anschluss an einen Vorfall Wiederherstellung leisten zu können, Mitarbeitersicherheitsmanagement zu betreiben und Schulungen der Mitarbeiter durchzuführen (vgl. [EUR23b], Art. 13 Abs. 1)). Die hierzu getroffenen Maßnahmen müssen in einem Resilienzplan festgehalten werden (vgl. [EUR23b], Art. 13 Abs. 2). Damit einher ergeht auch eine Verpflichtung, die nationale Aufsichtsbehörde, bei Vorfällen, binnen 24 Stunden zu unterrichten (vgl. [EUR23b], Art. 15). Im Falle der Nichterfüllung sieht die Richtlinie Sanktionen vor, welche jedoch von dem jeweiligen Mitgliedsstaat bis zum 17. Oktober 2024 in Eigenverantwortung zu erlassen sind und der Kommission mitzuteilen (vgl. [EUR23b], Art. 22).

Da es sich bei dieser Verordnung überwiegend um die physische Resilienz handelt, wurde simultan eine weitere Verordnung erlassen, welche sich mit digitaler Resilienz beschäftigt. Diese umfangreichere Verordnung wird in einem späteren Kapitel beleuchtet (vgl. 2.1.4).

2.1.4 Networks and Information Systems Directive

Die Verordnung (EU) 2022/2555, besser bekannt als die „NIS2“, ist 2023 innerhalb der Europäischen Union in Kraft getreten (vgl. [EUR23a]). Die Verordnung hat das Ziel, im Rahmen der europäischen Cybersicherheitspolitik[4], die Resilienz von Einrichtungen aus bestimmten Sektoren zu fördern und ein hohes gemeinsames Cybersicherheitsniveau der gesamten Union zu erreichen (vgl. [EUR23a], Art. 1 (1)).

Aus der Richtlinie ergehen einige Neuerungen. Angefangen bei den betroffenen Betreibern und Sektoren, gliedert die Verordnung Einrichtungen in zwei Gruppen, welche wiederum aus achtzehn Sektoren stammen (vgl. [EUR23a], Annex 1, 2). Hierzu werden die Begriffe „wesentliche Einrichtungen“ und „wichtige Einrichtungen“ eingeführt (vgl. [EUR23a], Art. 2, 3).

Wesentliche Einrichtungen werden unabhängig ihrer Größe als wesentlich angesehen, wenn einer der folgenden Punkte auf diese Einrichtung zutrifft:

1. Die Einrichtung überschreitet die Schwellenwerte für mittlere Unternehmen aus Empfehlung 2003/361/EG (vgl. [EUR24a], Anhang, Art.2 (1))

[4] CyberSicherheitspolitik. (n.d.). Gestaltung Der Digitalen Zukunft Europas. - https://digital-strategy.ec.europa.eu/de/policies/cybersecurity-policies [Zugriff: 10.03.2024]

2. Die Einrichtung ist ein qualifizierter Vertrauensdienstanbieter, Top-Level-Name-Registry Anbieter oder DNS-Dienstanbieter
3. Die Einrichtung ist ein Anbieter öffentlicher Kommunikationsnetze
4. Die Einrichtung ist eine Einrichtung der öffentlichen Verwaltung
5. Die Einrichtung wurde gemäß Art. 2 (2) b bis e als wesentliche Einrichtung eingestuft
6. Die Einrichtung wurde gemäß Richtlinie (EU) 2022/2557 (vgl. [EUR23b] als kritische Einrichtung eingestuft)

(vgl. [EUR23a], Art. 3 (1))

Einrichtungen, welche der Anhang 1 oder 2 aufgeführten Art entsprechen, jedoch nicht die Kriterien erfüllen, um als „wesentliche“ eingestuft zu werden, sind als „wichtig“ einzustufen (vgl. [EUR23a], Art. 3 (2)).

Die wichtigste und einschneidendste Änderung, im Rahmen dieser Verordnung, ist die Einführung von verpflichtenden Risikomanagementmaßnahmen für betroffene Unternehmen. So sind betroffene Unternehmen konkret dazu verpflichtet mindestens folgende Maßnahmen zu treffen:

1. Konzepte zur Risikoanalyse und Sicherheit von Informationssystemen
2. Bewältigungsmaßnahmen von Sicherheitsvorfällen
3. Business Continuity Maßnahmen
4. Sicherheit der Lieferkette, Sicherheit zwischen Einrichtungen, Dienstleistersicherheit
5. Sicherheit in der Entwicklung, Beschaffung und Wartung, inklusive Schwachstellenmanagement
6. Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit
7. Cyberhygiene und Schulungen zur Cybersicherheit
8. Konzepte für Kryptografie und Verschlüsselung
9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle
10. Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierung, gesicherte Kommunikation, ggf. gesicherte Notfallkommunikationssysteme

(vgl. [EUR23a], Art. 21 (2))

Ebenfalls wird eine Reform im Meldewesen eingeleitet. Hierzu sind betroffene Einrichtungen dazu verpflichtet die nationale Cybersicherheitsbehörde über signifikante Störungen zu unterrichten. In ausgewählten Fällen kann der Kreis der zu Informierenden um die Empfänger der Dienstleistungen erweitert werden (vgl. [EUR23a], Art. 23).

Auch auf die Regierungen der Mitgliedsstaaten kommen Pflichten zu. Zunächst sind diese dazu angehalten eine nationale Cybersicherheitsstrategie zu definieren und mit angemessener Aufsicht umzusetzen (vgl. [EUR23a], Art. 7). Weiterhin muss eine Aufsichtsbehörde ernannt werden, welche der nationale Ansprechpartner, in Fragen der Cybersecurity, ist (vgl. [EUR23a], Art. 8). Zusätzlich muss auf nationaler Ebene ein Rahmen für Cyberkrisenmanagement eingerichtet werden, damit im Falle von großen Sicherheitsvorfällen ein Plan zur Bewältigung besteht (vgl. [EUR23a], Art. 9). Betrachtet man den KRITIS-Sektor muss ein nationales Computer Security Incident Response Team (CSIRT) eingerichtet werden (vgl. [EUR23a], Art. 10). Damit die jeweilige nationale Cybersicherheitsbehörde ihre Pflichten ausüben kann, werden eine Vielzahl von notwendigen Befugnissen definiert, welche jedoch in dieser Arbeit nicht weiter beschrieben werden (vgl. [EUR23a], Art. 31).

In Verbindung mit den vorangegangenen Kapiteln und darin enthaltenen Verordnungen bietet diese Verordnung das Potenzial zu einem erhöhten Cybersicherheitsniveau beizutragen. Neben den betroffenen Einrichtungen, werden auch die Regierungen der jeweiligen Mitgliedsstaaten mit der Umsetzung verpflichtet, sodass diese in der gesamten Europäischen Union stattfinden wird. Die einzelnen Mitgliedsstaaten haben bis zum 17. Oktober 2024 Zeit, die Verordnung auf nationaler Ebene umzusetzen (vgl. [EUR23a], Art. 41). Weiteres zu der Umsetzung in Deutschland folgt in 2.2.2.

2.1.5 Europäische Datenschutzgrundverordnung

In der Informationssicherheit ist es von Vorteil möglichst viele Daten zu erheben und zu speichern, um im Nachgang weitreichende und umfassende Analysen durchzuführen. Dies kann jedoch schnell zu einem Konflikt führen, wenn man die EU-Datenschutzgrundverordnung (DGSVO) betrachtet.

Die DGSVO, vom 27. April 2016, ist eine Rechtsnorm, welche unmittelbar in allen Mitgliedsstaaten der Europäischen Union, ab dem 25. Mai 2018, Anwendung findet (vgl.[EUR23c], Art. 99). Die DGSVO besteht aus 173 zugrundeliegenden Beweggründen und 99 Artikeln. Übergeordnetes Ziel der DGSVO ist der Schutz von personenbezogenen Daten und die damit einhergehenden Rechte der zugehörigen Personen (vgl.[EUR23c], Art. 1 (1)).
Die DGSVO ist eine sehr umfassende Rechtsnorm, welche zwar nicht innerhalb des Betrachtungsraums, der vorliegenden Arbeit, veröffentlicht wurde, jedoch elementarer Bestandteil der Informationssicherheit, innerhalb der EU, ist.

Dies geht zweifelsfrei aus dem Anwendungsbereich hervor. Dieser wird zwei Arten unterteilt: der räumliche Anwendungsbereich und der sachliche Anwendungsbereich. Der räumliche Anwendungsbereich bezieht sich auf die Verarbeitung von personenbezogenen Daten, sofern die Tätigkeit eines Verantwortlichen oder eines Auftraggebers in der Europäischen Union erfolgt (vgl.[EUR23c], Art.3 (1)), die Daten einer Person zuzuordnen sind, welche sich in der Europäischen Union befindet (vgl.[EUR23c], Art.3 (2)) oder die Verarbeitung durch einen Verantwortlichen erfolgt, welche nicht in der Europäischen Union niedergelassen ist, jedoch dem Recht eines Mitgliedsstaates unterliegt (vgl.[EUR23c], Art.3 (3)). Bedeutender für die vorliegende Arbeit ist jedoch der sachliche Anwendungsbereich, welcher in Artikel 2 geregelt ist. Dieser beschäftigt sich mit der:

„*ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht-automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.*“ ([EUR23c], Art. 2 (1)).

Aufgrund der Definition von „personenbezogenen Daten“ (vgl.[EUR23c], Art.4 Satz 1) fallen diese technisch immer an, wenn ein System Merkmale, wie z.B. Browser-Cookies, IP-Adressen, Name, Adresse etc., speichert. Dementsprechend steht jedes Unternehmen, welches über Kundendaten verfügt, vor der Herausforderung eine Konformität mit der DGSVO zu erlangen. Durch die Implementierung von Maßnahmen zur Konformität mit bereits erwähnten bzw. noch zu erwähnenden Regulierungen, kann dies zu zusätzlichem Aufwand führen.

Wie bereits erwähnt, stellt dies ein sehr komplexes und schwieriges Thema dar. Dementsprechend wird im weiteren Verlauf der Arbeit keine Berücksichtigung der Rechtsnorm vorgenommen. Aufgrund der Wichtigkeit für den Themenbereich der Informationssicherheit wurde es jedoch für angebracht gehalten, eine kurze Beleuchtung der Rechtsnorm vorzunehmen.

2.2 Deutsche Regulierungen

Vor dem Hintergrund der bereits erwähnten europäischen Regulierungen, wurden ebenfalls nationale Regulierungen erlassen. Im Falle des KRITIS-Dachgesetzes und dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, dienen diese Regulierungen der Umsetzung des europäischen Gegenstücks. Nachfolgend werden diese Regulierungen analysiert und erläutert.

2.2.1 KRITIS-Dachgesetz

Das neue Kritis-Dachgesetz, oder auch KRITIS-DachG, tritt im Oktober 2024 in Kraft und stellt die nationale Umsetzung der CER-Richtlinie (vgl. 2.1.3) dar (vgl. [BUN24c]).

Im Fokus liegen hier die Betreiber „kritischer Anlagen“ aus den bisherigen KRITIS-Sektoren. Die Feststellung, ob ein Unternehmen ein solcher Betreiber ist, definiert sich über Schwellenwerte. Der Regelschwellenwert liegt hierbei bei 500.000 Empfänger (vgl. [BUN24c], §4). Mit der Annahme des Status, ein „Betreiber kritischer Anlagen“ zu sein, gehen Pflichten einher. Zunächst besteht für Betroffene eine Registrierungspflicht beim zuständigen Amt. Nach [BUN24c], §8 haben sich Betreiber kritischer Anlagen spätestens bis zum ersten Werktag der Inbetriebnahme zu registrieren. Weiterhin besteht die Pflicht, alle vier Jahre eine Risikoanalyse und Risikobewertung durchzuführen, mit dem Ziel interne sowie externe Risiken zu beurteilen (vgl. [BUN24c], §10). Sollte auf Grundlage der Risikoanalysen und Risikobewertungen oder anderen Informationen Handlungsbedarf bestehen, müssen Resilienzmaßnahmen in einem geeigneten und verhältnismäßigem Umfang getroffen werden. Konkret werden Maßnahmen gefordert, welche Vorfälle verhindern, physischen Schutz der Räumlichkeiten gewährleisten, auf Vorfälle reagieren, nach Vorfällen Wiederherstellung gewährleisten und das Personal sensibilisieren (vgl. [BUN24c], Anhang 1 (insbesondere zu berücksichtigende Maßnahmen nach §11 Abs 1)).

Diese Maßnahmen müssen in einem Resilienzplan vom Betreiber festgehalten werden und alle zwei Jahre dem zuständigen Amt zur Verfügung gestellt werden (vgl. [BUN24c], §11 (6)). Sollte es trotz Resilienzmaßnahmen zu einem Vorfall mit erheblichen Störungen kommen, hat der Betreiber unverzüglich, spätestens 24 Stunden nach dem Vorfall, dem zuständigen Amt eine Meldung zuzustellen und spätestens einen Monat nach dem Vorfall, einen ausführlichen Bericht zu übermitteln (vgl. [BUN24c], §12).

Das angesprochene zuständige Amt wird hierbei das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) sein. Neben umfangreichen Aufsichtskompetenzen, werden dem BBK durch die Zusammenarbeit mit dem BSI und der Bundesanstalt für Finanzdienstleistungsaufsicht (Bafin) Informationen, zur Ausführung der Pflichten, zur Verfügung gestellt (vgl. [BUN24c], §3).

Durch das KRITIS-Dachgesetz wird die bestehende KRITIS-Verordnung abgeändert und stellt zusammen mit dem NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (vgl. 2.2.2) einen nächsten und wichtigen Schritt in Richtung einer hohen Resilizenz der Bundesrepublik dar.

2.2.2 NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

Das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, oder auch „NIS2UmsuCG“, tritt im Oktober 2024 gemeinsam mit dem KRITIS-Dachgesetz (vgl. 2.2.1) in Kraft (vgl. [BUN24b]). Wie der Name bereits anmuten lässt, handelt es sich um ein Gesetz mit zwei übergestellten Zielen. Zum einen setzt es die NIS2-Richtlinie (vgl. 2.1.4) um und zum anderen wird die Gesetzeseinführung von der Bundesregierung genutzt, um dem BSI, welches als nationale Aufsichtsbehörde fungiert (vgl. [BUN24b], §1), weitere Befugnisse zu erteilen. Da in dem Kapitel 2.1.4 bereits die übergeordnete Richtlinie erläutert wurde, werden in diesem Abschnitt lediglich abweichende Punkte aufgegriffen.

Angefangen bei dem Anwendungsbereich werden in der nationalen Umsetzung, zusätzlich zum europäischen Vorbild (vgl. [EUR23a], Art. 2, 3), die kritischen Anlagen separat in die „besonders wichtigen Einrichtungen “ aufgenommen (vgl. [BUN24b], §28). Zusätzlich, zu den in diesem Gesetz vorgeschriebenen Pflichten, gelten für diese die Pflichten aus dem KRITIS-Dachgesetz (vgl. 2.2.1). Die Umsetzung der in der NIS2-Richtlinie geforderten Risikomanagementmaßnahmen wird in diesem Gesetz ohne signifikante Änderung übernommen (vgl. [BUN24b], §30). Zusätzlich ergehen aus NIS2UmsuCG Pflichten für Leitungsorgane der betroffenen Einrichtungen. So sind diese dazu verpflichtet die Umsetzung der geforderten Risikomanagementmaßnahmen zu billigen und zu überwachen (vgl. [BUN24b], §38). Es wird, im Rahmen des Nachweis- und Prüfungswesen, eine Unterteilung vorgenommen. Während Betreiber kritischer Anlagen alle drei Jahre einen Nachweis über die Einhaltung der Risikomanagementmaßnahmen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) erbringen müssen (vgl. [BUN24b], §39 (2)), müssen besonders wichtige Einrichtungen dies nur auf Nachfrage, durch das BSI, erbringen (vgl. [BUN24b], §64). Noch abgeschwächter ist dieser Vorgang bei den wichtigen Einrichtungen. Diese werden nur „anlassbezogenen Nachweisprüfungen“ unterzogen (vgl. [BUN24b], §65).

Damit das BSI seinen Aufsichtspflichten nachgehen kann, werden diese umfangreichen Kompetenzen zugesprochen. Konkret kann das BSI, nach diesem Gesetz, bei besonders wichtigen Einrichtungen:

- Zu Prüfungen und Audits verpflichten (vgl. [BUN24b], §64 (1))
- Maßnahmen, zur Verhütung von Sicherheitsvorfällen dienen, erlassen (vgl. [BUN24b], §64 (2))
- Verbindliche Anweisungen, zur Umsetzung der Verpflichtungen, erlassen und die Einrichtungen über Abwehrmaßnahmen unterrichten (vgl. [BUN24b], §64 (3), (4))
- einen Überwachungsbeauftragen ernennen (vgl. [BUN24b], §64 (5))
- den Einrichtungen Genehmigungen entziehen und dem Leitungsorgan eine Wahrnehmungsuntersagung von Leitungsaufgaben erteilen (vgl. [BUN24b], §64 (6))

Im dem Fall von wichtigen Einrichtungen ist das BSI befugt, ähnliche Maßnahmen zu ergreifen, welche jedoch in ihrer Form der niedrigeren Kritikalität angepasst sind (vgl. [BUN24b], §65).

Für Bundeseinrichtungen, als besonders wichtige Einrichtungen, bestehen ebenfalls die Pflichten Risikomanagementmaßnahmen, Meldepflichten, Registrierungspflichten, Nachweispflichten , Unterrichtungspflichten und Überwachungspflichten. Weitaus interessanter sind hier jedoch Pflichten, welche die Steuerung der Informationssicherheit innerhalb der Bundesregierung, betreffen. So ist diese verpflichtet eine Bundes-Chief-Information-Security-Officer zu ernennen, welche die Koordination der Informationssicherheit auf Bundesebene koordiniert (vgl. [BUN24b], §48-§50). Weiterhin muss für Einrichtungen der Bundesverwaltung ein Informationssicherheitsbeauftragter ernannt werden, welcher für den Aufbau und die Aufrechterhaltung des Informationssicherheitsprozesses der Einrichtung verantwortlich ist (vgl. [BUN24b], §45) und die jeweiligen Informationssicherheitsrichtlinien für

das Ressort fortschreibt (vgl. [BUN24b], §64). Zusätzlich hierzu muss für jedes große Digitalisierungsvorhaben ein eigener Informationssicherheitsbeauftragter bestellt werden (vgl. [BUN24b], §47).

Wie aus diesem Kapitel hervorgeht, wird mit diesem Gesetz nicht nur die Umsetzung der NIS2-Richtlinie fokussiert, sondern auch die Chance genutzt, um speziell auch innerhalb der Bundesregierung den Informationssicherheitsprozess zu modernisieren und dem BSI mit mehr Befugnissen auszustatten.

2.2.3 BSI-Gesetz

Das *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*, bzw. BSI-Gesetz oder BSIG, ist ein deutsches Bundesgesetz, welches die Rechtsgrundlage für das BSI darstellt und Pflichten zum Schutz von informationstechnischen Systemen regelt. Das BSI geht nach diesem Gesetz als nationale Cybersicherheitsbehörde hervor und erfüllt diesbezüglich Pflichten. Diese Pflichten werden in §3 BSIG definiert. Weiterhin werden in den darauf folgenden weitreichende Befugnisse eingeräumt, um jene Pflichten mit fundierter Rechtsgrundlage zu erfüllen (vgl. BSIG §1 bis §8; §9).

Der für die vorliegende Arbeit deutlich interessantere Teilbereich des BSIG ist jedoch die Definition von Anforderungen an kritische Infrastrukturen. Die Intention hinter diesem Teil besteht darin, betroffene Unternehmen widerstandsfähiger zu machen. So will *„Der Gesetzgeber will, dass etwa [...] [kritische Infrastrukturen] im Kontext mit digitalen Prozessen sicherstellen, dass sie vor Angriffen über Netzwerke (Cyberangriffe) geschützt sind und jederzeit - trotz fortschreitender Technisierung und Digitalisierung - in der Lage sind, die [...]sicherheit zu gewährleisten.“*([JOR20], S.82).

Das BSI-Gesetz gibt keine konkreten Anforderungen für betroffene Unternehmen an. Das Gesetz spricht in §8a lediglich von der Verwendung von *„angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen [...]“* ([BSI], §8a (1)) und einer damit einhergehenden Nachweispflicht (vgl. [BSI], §8a (2)). Weiterhin wird in §8a (1a) eine Pflicht zum Einsatz von Systemen zur Angriffserkennung gegeben. Zur Spezifizierung von §8a hat das BSI gemeinsam mit dem Fachausschuss für Informationstechnologie (FAIT) des Instituts für Wirtschaftsprüfer in Deutschland e.V. (IDW) einen Anforderungskatalog für KRITIS-Betreiber und Prüfer bereitgestellt. Hier werden 100 Anforderungen bzw. Kriterien für Prüfer angegeben (vgl. [BUN20b]).

Dieses Dokument wird als Grundlage für die weitere Bearbeitung der vorliegenden Arbeit, in Bezug auf Anforderungen des BSIG, verwendet.

2.3 Dokumentation der Mindestanforderungen

Die vorstehenden Kapitel dienen dem Überblick über die jeweiligen Gesetze bzw. Verordnungen. Es wurden nicht alle spezifischen Anforderungen genannt. Es ist jedoch von essenzieller Bedeutung die geforderten Mindestanforderungen zu identifizieren. Durch die Analyse der jeweiligen Verordnungen wird klar, dass innerhalb dieser nur teilweise konkrete Anforderungen festgehalten werden. Überwiegend erfolgt die Bekanntmachung von technischen Maßnahmen zur Konformität über delegierte Rechtsakte.

Für eine transparente und nachvollziehbare Dokumentation wurde ein tabellarischer Ansatz gewählt (vgl. 2.3). Die Tabelle ist in mehrere Spalten unterteilt, namentlich:

- Verordnung
- Kennung
- Fundstelle
- Beschreibung

Die ersten drei Spalten dienen der Identifikation der Anforderung. Wichtig hierbei zu erläutern ist die Struktur der „Kennung“. Diese setzt sich jeweils aus dem Kürzel des Gesetzes bzw. der Verordnung und einer Nummer zusammen. Die Nummer wird dabei nach Anwendungsfeld unterteilt. Ein Beispiel hierfür sind Anforderungen aus dem CRA (vgl. 2.1.1). Hier werden die Anforderungen, welche den Einführer betreffen in CRA.1.X festgehalten und die Anforderungen, welche den Händler betreffen in CRA.2.X.

Verordnung	Kennung	Fundstelle	Beschreibung
CRA	CRA.1.1	Art. 13 (1) (3)	Einführer dürfen Produkte mit digitalen Elementen nur in Verkehr bringen, wenn diese den Anforderungen aus Anhang 1 Abs. 1 genügen und wenn die vom Hersteller festgelegten Verfahren den Anforderungen aus Anhang 1 Abs. 2 genügen. Sofern von einem Produkt ein erhebliches Cybersicherheitsrisiko ausgeht, müssen der Hersteller und die Martküberwachungsbehörde informiert werden.

Tabelle 2.3: Beispielausschnitt: Anhang A

3 Analyse von relevanten Normen und Standards

Das nachfolgende Kapitel dient dem Zweck, dem Leser eine Einleitung in etablierte nationale und internationale Standards und Normen zu erteilen. Dies stellt die Verständnisgrundlage dar, um im Anschluss eine fundierte Zuordnung der Standards durchzuführen. Es werden konkret drei etablierte Standardwerke thematisiert. Diese sind namentlich die internationale Norm ISO27k und die beiden nationalen Standardwerke BSI C5 und der BSI IT-Grundschutz.

3.1 ISO27k-Normenreihe

Die Internationale Orgranisation für Normung (ISO) und die International Electrotechnical Commission (IEC) haben mit ihrer ISO27k-Normenreihe ein umfassendes Werkzeug geschaffen, welches zur Implementierung von Informationssicherheitsmanagementsystemen (ISMS) von Nutzen ist. Im nachfolgendem Kapitel wird zunächst ein Gesamtüberblick über die ISO-Reihe gegeben und im Anschluss die ISO27001 und ISO27002 konkretisiert.

3.1.1 Überblick

Die ISO27k-Normenreihe basiert auf dem britischen Standard (BS) 7799 aus den Jahren 1999/2002. Ziel dieser Normenreihe ist die Implementierung von ISMS (vgl.[DEU], S.6). Hierzu besteht die Normenreihe inzwischen aus mehr als 50 Einzelnormen.

Die Abb. 3.1 zeigt den strukturellen Aufbau der für ISMS relevanten Normen der Normenreihe. Wie zu erkennen ist, ist der ISMS-Normenteil in fünf Bereiche unterteilt. Namentlich sind diese Bereiche: „Begriffsnormen“, „Anforderungsnormen“, „Leitfadennormen“, „sektorspezifische Leitfadennormen“ und „maßnahmenbezogene Leitfadennormen“.

Die **Begriffsnorm** ISO/IEC 27000 definiert grundlegende Begriffe und Konzepte von ISMS, welche im Kontext der Normenreihe Anwendung finden (vgl.[DEU], S.7-19). Die **Anforderungsnormen** stellen grundlegende Anforderung an Art und Ausführung eines ISMS. Im Rahmen des ISMS-teils der Normenreihe sind dies die ISO/IEC 27001, welche im Kapitel 3.1.2 tiefer behandelt wird, die ISO/IEC 27006 und die ISO/IEC 27009. **Leitfadennormen** stellen, wie der Name schon sagt, Leitfäden zur Umsetzung und Implementierung der geforderten Maßnahmen dar. Da verschiedene Branchen auch verschiedene Ansätze zur Umsetzung benötigen, gibt der ISMS-Normenteil hierfür konkretisierende Umsetzungshinweise in den **sektorspezifischen Leitfadennormen** (vgl.[DEU], S.30-36).

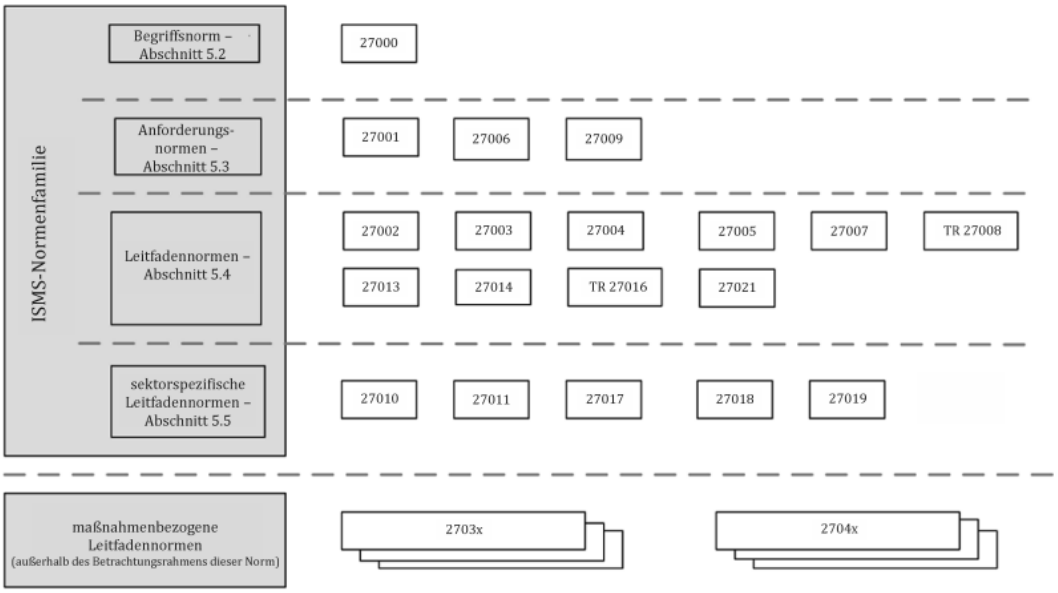

Abbildung 3.1: Zusammenhänge der ISMS-Normenfamilie
(Quelle: [DEU], S.29)

3.1.2 ISO27001

Die ISO/IEC 27001 ist die, aus der britischen Standards BS 7799-2 Norm überführte, Basisnorm der ISO27k-Familie. Sie besteht aus zehn Kapiteln und Anhang. Zum Jahr 2022 haben sich weltweit bereits über 70.000 Unternehmen mit dieser Norm zertifizieren lassen, was den Hauptgrund für die Auswahl als relevanten Standard für die Arbeit gewesen ist (vgl.[STA24]).

Die ersten drei Kapitel sind lediglich zur Abgrenzung des Anwendungsbereichs, Verweise auf andere Normen und Begriffe, vorhanden (vgl.[DEU24a], S.6ff). Im Hauptteil der Norm werden Anforderungen an ein ISMS definiert (vgl.[DEU24a], Kapitel 4-10). Anhand dieser Anforderungen werden Voraussetzungen beschrieben, welche für den Aufbau, Implementierung und Instandhaltung eines ISMS berücksichtigt werden müssen. **Kapitel vier**, *Kontext der Organisation*, besteht aus vier Unterkapiteln. Es beschäftigt sich einen ganzheitlichen Überblick über das Unternehmen, eigene Ziele und Ziele externer Parteien zu verstehen und den Anwendungsbereich des ISMS abzugrenzen, um Anforderungen an das ISMS abzuleiten (vgl.[DEU24a], S.7f). Im Anschluss wird in **Kapitel fünf**, *Führung*, der Vorstand betrachtet. Es werden in den drei folgenden Unterkapiteln vor allem Verpflichtungen in Hinsicht auf die Führung und Führungspolitik thematisiert (vgl.[DEU24a], S.8f). Ziel hierbei ist es, charakteristische Elemente einer Führungsperson herauszustellen, welche zu einer „guten Führung“ führt (vgl.[KER23], S.40f). Es wird die ultimative Verantwortung der obersten Leitung, für Erfolg oder Misserfolg des ISMS, herausgestellt. Das **sechste Kapitel**, *Planung*, dient dem vorwiegenden Zweck, zwei zentrale Prozesse der Norm zu etablieren. Hierbei handelt es sich um die Informationssicherheitsrisikobeurteilung und die Informationssicherheitsrisikobehandlung (vgl.

[DEU24a], Kap. 6.1.2-6.1.3). Zur Etablierung des Ersteren, gibt die Norm eine Reihe von Rahmenbedingungen vor, schreibt jedoch keinen konkreten Umsetzungsansatz vor – Art der Umsetzung obliegt der jeweiligen Organisation (vgl. [KER23], S.50). Für Zweiteres erfolgt anhand von sechs einzuhaltende Kriterien (Auswahl von Behandlungsoptionen, Festlegung von Maßnahmen, Gegenüberstellung der ausgewählten Maßnahmen mit Anhang A, Erstellung einer Anwendbarkeitserklärung, Erstellung eines Planes zur Risikobehandlung, Genehmigung des Planes) eine leichte Vorgabe zur Etablierung (vgl. [DEU24a], Kap. 6.1.3 a-f). Weiterhin werden in diesem Kapitel neben Informationssicherheitszielen und dessen Erreichung, die Planung von Änderungen thematisiert (vgl. [DEU24a], Kap. 6.2 und 6.3). Zur Erfüllung der bisherigen Arbeitsprozesse werden Mittel benötigt. Zu diesem Zweck wird in **Kapitel sieben**, *Unterstützung*, die Ressourcenverwaltung betrachtet. Hierzu werden überwiegen nicht-monetäre Ressourcen, wie Kompetenzen, Sicherheitsbewusstsein, Kommunikation und dokumentierte Informationen, thematisiert (vgl. [KER23], S.63). Im **achten Kapitel**, *Betrieb*, wird zunächst im ersten Unterkapitel die betriebliche Planung und Steuerung thematisiert. Im Anschluss werden die im vorherigen Kapitel erstellten Kernprozesse, während des Betriebs, betrachtet (vgl. [DEU24a], S.14). Dieses Kapitel dient dem Zweck, die bisherige Planung umzusetzen (vgl. [KER23], S.71). Das darauffolgende **Kapitel neun**, *Bewertung der Leistung*, beschäftigt sich mit dem Prozess, wie man die Leistung des ISMS, anhand von Kennzahlen, messen kann. Hierzu werden die Überwachung, Messung, Analyse und Bewertung; internes Auditing; und die Managementbewertung herangezogen (vgl. [DEU24a], Kap. 9).
Zuletzt wird im **Kapitel zehn**, *Verbesserung*, ein fortlaufender Verbesserungsprozess und Korrekturmaßnahmen bei Nichtkonformität beschrieben (vgl. [DEU24a], Kap. 10).

Der jedoch weitaus wichtigere Teil der Norm befindet sich im Anhang. Im Anhang werden konkrete „Controls“ angeführt, welche Maßnahmen darstellen. Zum aktuellen Zeitpunkt definiert die Norm 93 Controls. Die Controls gliedern sich dabei in die thematischen Gruppen „Organisatorische Maßnahmen“, „Personenbezogene Maßnahmen“, „Physische Maßnahmen“ und „Technologische “ Maßnahmen(vgl.[DEU24a], Anhang A). Abb. 3.2 zeigt eine Übersicht die ISO/IEC 27001.

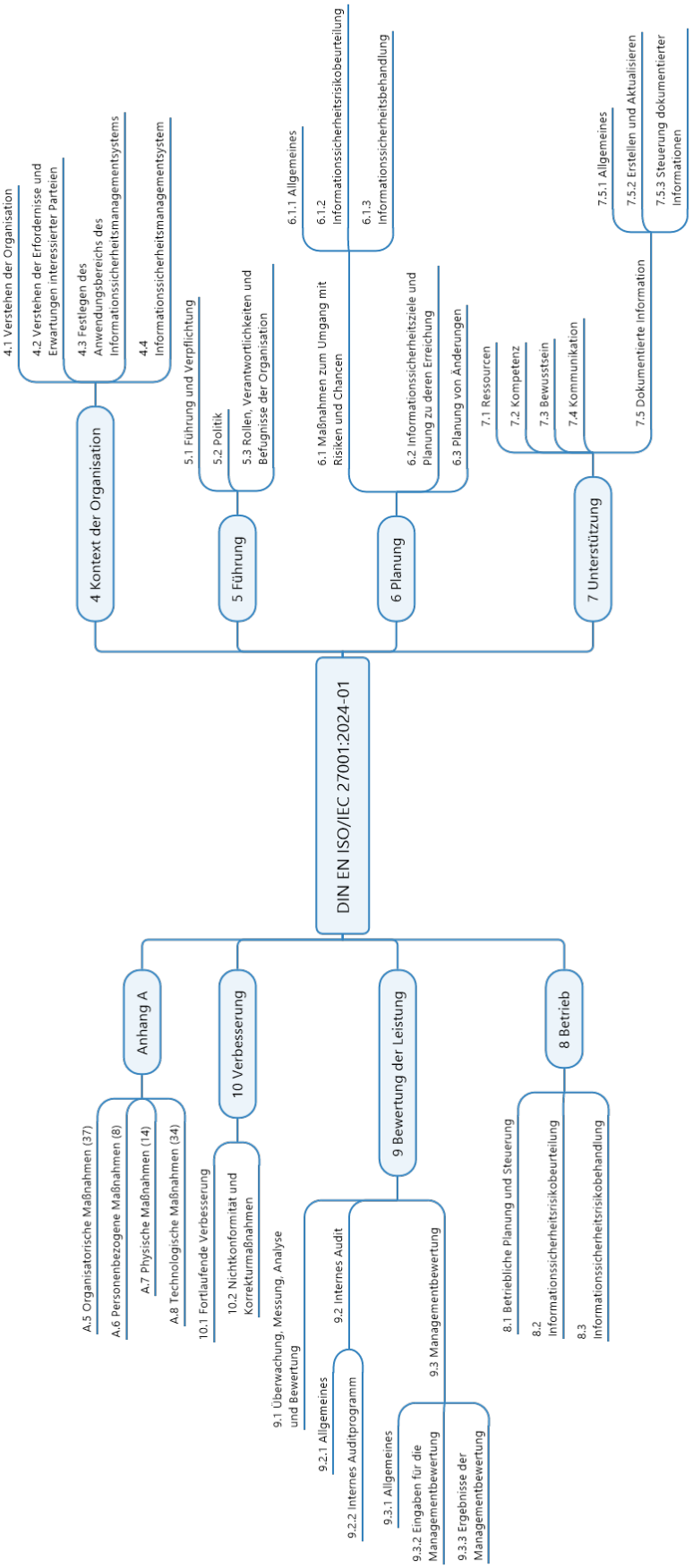

Abbildung 3.2: ISO/IEC 27001: Überblick
(Quelle: Eigene Darstellung nach [DEU24a])

3.1.3 ISO27002

Ein ISMS verfolgt dem Zweck eine ganzheitliche Betrachtung von Risiken innerhalb einer Organisation, in Bezug auf Informationssicherheit (vgl. 3.1.2). Da jedes Unternehmen sich in Größe, Art und Branche unterscheidet, fallen die zu wählenden Sicherheitsmechanismen unterschiedlich aus und es gilt die richtigen zu wählen. Die ISO/IEC 27001 bietet eine Reihe von Controls an, welche sicherstellen sollen, dass Informationssicherheit gegeben ist, sofern diese richtig implementiert worden sind. Die ISO/IEC 27001 bietet jedoch keine genauen Erläuterungen, was welche Control bewirkt. Hier kommt die **ISO/IEC 27002** ([DEU24b]) ins Spiel.

Die ISO/IEC 27002 stellt eine zusätzliche Norm dar, welche dieses Problem adressieren soll und Anleitung zur Auswahl von geeigneten Maßnahmen bietet (vgl. [VIE22], S.30; [NAS24], S.183f). Um dies zu bewerkstelligen, kategorisiert die Norm die Controls (aus [DEU24a], Annex), anhand von:

- **Maßnahmenart** (Präventiv, Detektiv, Korrektiv)
- **Informationssicherheitseigenschaft** (Vertraulichkeit, Integrität, Verfügbarkeit)
- **Cybersicherheitskonzept** (Identifizieren, Schützen, Erkennen, Reagieren, Wiederherstellen)
- **Betriebsfähigkeit** (Governance, Asset Management, Informationsschutz, Sicherheit der Humanressourcen, physische Sicherheit, System- und Netzwerksicherheit, Anwendungssicherheit, sichere Konfiguration, Identitäts- und Schwachstellenmanagement, Aufrechterhaltung, Sicherheit in Lieferantenbeziehungen, Recht und Compliance, Handhabung von Informationssicherheitsereignissen und Vertrauenswürdigkeit in Bezug auf die Informationssicherheit),
- **Sicherheitsdomänen** (Governance und Ökosystem, Schutz, Verteidigung, Resilienz)

(vgl. [DEU24b], 4.3)

Durch diese Ausgestaltung und tiefgehender Erklärung, bietet diese Norm eine solide Grundlage, um ein tiefgehendes Verständnis zur Auswahl der passenden Controls zu erlangen.

3.2 BSI IT-Grundschutz

Der IT-Grundschutz, des Bundesamts für Sicherheit in der Informationstechnik (BSI), stellt ein umfassendes Werkzeug, zur Erarbeitung einer ganzheitlichen Absicherungsstrategie, zum Schutz von Informationssystemen und -infrastrukturen, dar. Kernbestandteile des BSI IT-Grundschutzes sind vier Standards und das IT-Grundschutz-Kompendium[1]. Nachfolgend werden die aufgezeigten Bestandteile thematisiert.

[1] IT-Grundschutz. (n.d.) - https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz$_{n}$ode.html[Zugriff: 10.03.2024]

3.2.1 BSI 200-1

Der BSI-Standard 200-1 „Managementsysteme für Informationssicherheit (ISMS)“ beschreibt, wie ein Informationssicherheitsmanagementsystem aufzubauen ist. Hierfür werden Komponenten und Prozesse, welche in einem ISMS vorhanden sein müssen, aufgezeigt (vgl. [BUN17a], S. 15-19). Um funktional zu sein, braucht ein ISMS stets eine ausreichende Menge an monetären, personellen und zeitlichen Ressourcen (vgl. [BUN17a], S.26f). Weiterhin wird ausführlich beschrieben, welche Rolle die Leitungsebene der Institution dabei übernehmen muss, damit das ISMS im ganzen funktional ist und kontrolliert wird (vgl. [BUN17a], S.20-25). Die Gesamtverantwortung bei der Informationssicherheit obliegt stets der Leitungsebene. Diese muss hierzu eine Informationssicherheitsleitlinie erarbeiten und auch entsprechend kommunizieren. Die Leitlinie sollte dabei transparent darlegen, anhand welcher Maßnahmen und Strukturen die Informationssicherheit innerhalb der Institution gewahrt wird (vgl. [BUN17a], S. 19f). Zuletzt wird der Sicherheitsprozess und Lebenszyklus eines Sicherheitskonzepts, von der Planung über die Erstellung, bis hin zur Erfolgskontrolle, thematisiert (vgl. [BUN17a], S.28-38).

3.2.2 BSI 200-2

Der BSI-Standard 200-2 beschreibt das konkrete Vorgehen, also die Methodik, des IT-Grundschutzes (vgl. [BUN17b]). Vorangehend, an den Kernbestandteil dieses Dokuments, wird in Kapitel 3 bis 5 erneut der Sicherheitsprozess detailliert erläutert. Darauffolgend werden die drei Vorgehensmodelle (s. 3.3) der IT-Grundschutz-Methodik erläutert, die „Basis-Absicherung“, die „Standard-Absicherung“ und die „Kern-Absicherung“ (vgl. [BUN17b], Kap. 6-8).

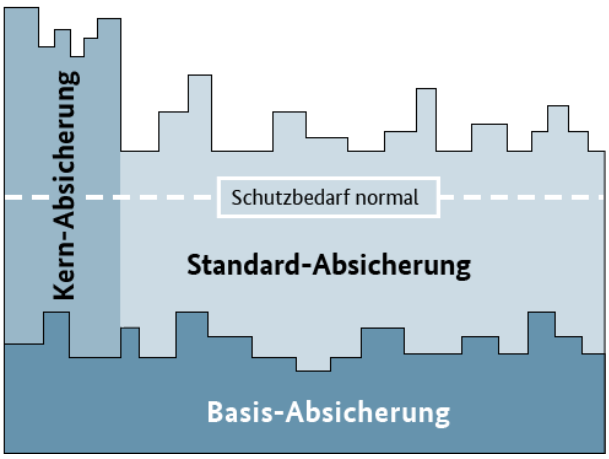

Abbildung 3.3: Die drei IT-Grundschutz-Absicherungsvarianten ([BUN22])

Die **Basis-Absicherung** stellt das Einstiegsvorgehen dar und zeichnet sich durch einen verhältnismäßig geringem Aufwand zur Einführung aus. Ziel ist es hierbei ein breites Grundniveau zu schaffen. Das allgemeine Vorgehen gliedert sich hierbei in die Definition des Geltungsbereiches, Priorisierung des Informationsverbundes, IT-Grundschutz-Check, Realisierung und der Auswahl des weiteren Vorgehens aus (vgl. [BUN17b], S.61f). Bei der Auswahl dieser sollte die Basis-Absicherung nicht als endlicher Prozess gesehen werden, sondern als Fundament, um darauf aufbauend weiteres Vorgehen anzustreben. Das BSI empfiehlt diese Art der Absicherung, wenn:

- die Umsetzung der Informationssicherheit noch in den Anfängen steht
- die Geschäftsprozesse kein deutlich erhöhtes Gefährdungspotenzial aufweisen
- das angestrebte Sicherheitsniveau normal ist
- der Diebstahl, die Zerstörung oder Kompromittierung von Assets existenzbedrohenden Schaden nach sich führt
- kleinere Sicherheitsvorfälle tolerierbar sind (vgl. [BUN17a], S.29)

Sollte eine Institution besonders schützenswerte Assets besitzen und deren Verlust existenzbedrohend sein können, kann eine **Kern-Absicherung** ein valides Mittel zur Vorbeugung sein. Da bei diesem Vorgehen davon ausgegangen wird, dass die betrachteten Assets einen gewissen Schutzbedarf innehaben, werden Assets durch eine Strukturanalyse in Kategorien eingeteilt. Es ist davon auszugehen, dass sich, die für dieses Vorgehensmodell relevanten Assets, in der höchsten Kategorie ansiedeln. Daraus resultierend können „Kronjuwelen“ bestimmt werden (vgl. [BUN17b], S. 72f). Da die Absicherung dieser stets mit einem erhöhten finanziellen Aufwand einhergehen, fällt die Bestimmungsaufgabe in den Bereich der Leitungsebene (vgl. [BUN17b], S. 71). Weiterhin gilt, dass dieses Vorgehen keine endliche Lösung darstellt. Auch hier sollten weitere Maßnahmen getroffen werden, um eine ganzheitliche Absicherung der Institution zu schaffen. Das BSI empfiehlt die Kern-Absicherung, wenn:

- Nur ein kleiner Teil der Geschäftsprozesse einen deutlichen erhöhten Schutzbedarf innehaben
- Die betroffenen Geschäftsprozesse zügig identifiziert und eindeutig eingegrenzt werden können
- eindeutig benennbare Assets vorhanden sind, deren Diebstahl, Zerstörung oder Kompromittierung einen existenzbedrohenden Schaden nach sich führt
- kleinere Sicherheitsvorfälle tolerierbar sind (vgl. [BUN17a], S.29)

Die **Standard-Absicherung** stellt das effektivste Vorgehensmodell der IT-Grundschutz-Methodik dar, um eine ganzheitliche und tiefgehende Informationssicherheit zu bewerkstelligen. So ist dieses im Regelfall das Ziel, wenn der IT-Grundschutz in der Institution etabliert werden soll. Um eine ganzheitliche und umfassende Informationssicherheit zu etablieren, wird das IT-Grundschutz-Kompendium herangezogen, welches über eine Vielzahl von Bausteinen verfügt, um eine breite Anzahl von Szenarien abzudecken (vgl. [BUN17b, S.78]). Damit diese Bausteine unmittelbar auf die Assets angewendet werden können erfolgt eine Auflistung aller Assets. Um diesen Prozess effektiv zu gestalten, können

diese nach Merkmalen gruppiert werden. Nach Gruppierung und Risikoanalyse können die Bausteine individuell den Assets oder Gruppen zugewiesen werden. Das BSI empfiehlt die Standard-Absicherung, wenn:

- die Institution bereits mit dem IT-Grundschutz arbeitet
- bereits Sicherheitskonzepte nach IT-Grundschutz oder ISO 27001 erstellt wurden
- der Reifegrad der Informationssicherheit in der Institution bereits angemessen ist, sodass keine Erst-Absicherung notwendig ist
- es kein Handlungsbedarf besteht, einzelne Geschäftsprozesse vordringlich abzusichern
- keine Assets vorhanden sind, deren Diebstahl, Zerstörung oder Kompromittierung keinen existenzbedrohenden Schaden nach sich führt
- Sicherheitsvorfälle nicht akzeptabel sind, jedoch keinen existenzbedrohenden Schaden nach sich führen (vgl. [BUN17a], S.30)

3.2.3 BSI 200-3

In den verschiedenen IT-Grundschutz-Methodiken ist unter anderem die Rede von „Risikoanalysen“. Der BSI-Standard 200-3 thematisiert dies und zeigt den Weg auf, wie diese Analyse durchzuführen ist.

Zunächst sind mithilfe des IT-Grundschutz-Kompendiums die Gefährdungen zu erfassen, welche für die betrachteten Assets in Erscheinung treten können (vgl. [BUN17c], S.16). Im Anschluss erfolgt die Risikobewertung anhand von Eintrittshäufigkeit und Schadensauswirkungen. Die Eintrittshäufigkeit wird in dem Standard in die vier Kategorien „gering“, „mittel“, „hoch“ und „sehr hoch“, aufgeteilt, während die Schadensauswirkung in die Kategorien „vernachlässigbar“, „begrenzt“, „beträchtlich“ und „existenzbedrohend“ (vgl. [BUN17c], S.26f) aufgeteilt wird. Dies führt wiederum zu einer Matrix, welche in Abbildung 3.4 zu sehen ist. Nach Ermittlung der Risiken muss festgelegt werden, wie mit diesen umgegangen wird (vgl. [BUN17c], Kap. 6).

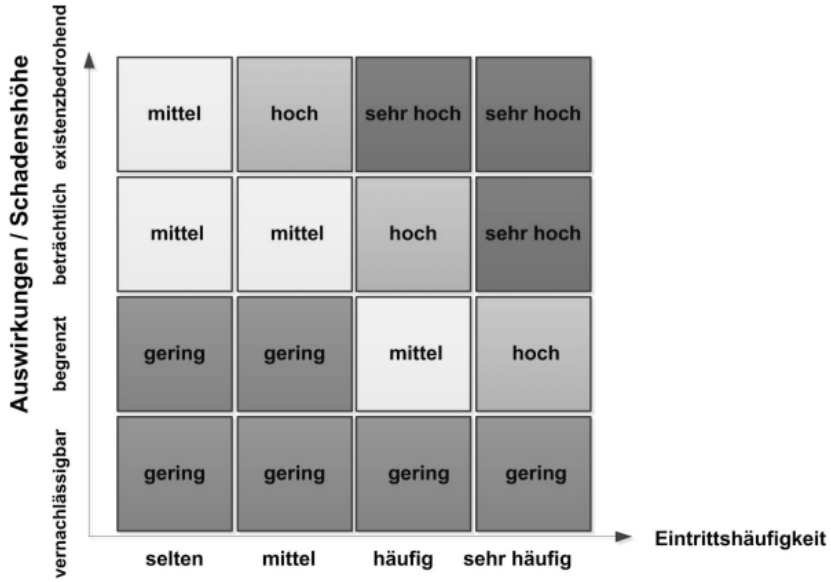

Abbildung 3.4: Matrix zur Einstufung von Risiken, nach BSI-Standard 200-3 ([BUN17c], S.27)

Gefundene Risiken müssen behandelt werden. Dabei können die Ursachen, wenn möglich ausgeschlossen werden, Eintrittshäufigkeiten können verringert werden, Auswirkungen abgeschwächt und finanzielle Schäden können durch Versicherungen transferiert werden. Danach verbleibende Risiken müssen bewusst akzeptiert werden (vgl. [BUN17c], S.32-34).

3.2.4 BSI 200-4

Komplettiert wird die Standardreihe durch einen Standard zum Notfallmanagement. Es besteht immer die Frage, was passiert, wenn es trotz Absicherung zu einem Sicherheitsvorfall kommt. Der BSI-Standard 200-4 ist hierbei laut BSI besonders für unerfahrene Business-Continuity-Anwendern hilfreich. Mit diesem Standard wird eine praxisnahe Anleitung zur Verfügung gestellt, um eine Business Continuity Management System (BCMS) aufzubauen. Zudem wird ein Anforderungskatalog zur Verfügung gestellt, welcher Erklärungen und konkrete Anforderungen an ein solches System liefert (vgl. [BUN23a], S.13f).

3.2.5 BSI IT-Grundschutz-Kompendium

Neben der Standardreihe stellt das IT-Grundschutz-Kompendium einen essenziellen Teil des IT-Grundschutzes dar. Das Kompendium behandelt drei elementare Teilbereiche (Einstieg und Hinweise zum Schichtenmodell, elementare Gefährdungen, Bausteine).

Der Teilbereich „Einstieg und Hinweise zum Schichtenmodell“ stellt den einleitenden Teil des

Kompendiums dar. Hier folgen Beschreibungen zu der Idee, der Zielsetzung und der Struktur des Kompendiums. Weiterführend werden Hinweise erteilt, wie aus der 858 Seiten langen Monografie, die richtigen Bausteine ausgewählt werden können. Im Anschluss werden elementare Gefährdungen thematisiert. Das Kompendium führt 47 dieser Gefährdungen, welche:

- für die Risikoanalyse optimiert sind
- Neutralität in Bezug auf Produkte und Technik wahren
- Kompatibel zu internationalen Katalogen sind
- sich nahtlos in den IT-Grundschutz einfügen lassen

(vgl. [BUN23b], Gesamtinhaltsverzeichnis)

Den Großteil des Kompendiums machen jedoch die Bausteine aus, welche in Schichten organisiert sind (vgl. 3.5). Hierbei sind die Bausteine in „Prozess-Bausteine“ und „System-Bausteine“ aufgeteilt, welche jeweils unterschiedliche Schichten beinhalten. Prozess-Bausteine werden auf den gesamten bzw. große Teile des Informationsverbundes angewendet, während die System-Bausteine auf ein einzelne oder gruppierte Zielobjekte angewendet werden (vgl. [BUN23b], S.1f). Als Beispiel für einen Prozess-Baustein kann ORP „Organisation und Personal“, mit ORP.1 „Organisation“, betrachtet werden. ORP.1 befasst sich im Kern mit allgemeinen Anforderungen an die Institution, welche in Summe zu einer Erhöhung der Informationssicherheit beitragen, wie z.B. die Festlegung von Verantwortlichkeiten und Rollen (ORP.1.A1) oder der Erstellung einer Richtlinie zur sicheren IT-Nutzung (ORP.1.A16) (vgl. [BUN23b], ORP.1, S.1). Hingegen befasst sich NET.1.1 „Netzarchitektur und -design“ mit dem Gesamtnetz als Zielobjekt und stellt so grundlegende Anforderungen an die Konzeption und den Betrieb von kabelgebundenen Netzen und Datenkommunikation (vgl. [BUN23b], NET.1.1, S.1). Unabhängig von der Art der betrachteten Bausteine, sind diese jeweils mit Einleitung und Abgrenzung zu anderen Bausteinen, Gefährdungslage, Anforderungen für die Basis-Absicherung, Anforderungen für die Standard-Absicherung und ggf. Anforderungen für einen erhöhten Schutzbedarf dokumentiert.

Weiterhin werden die Anforderungen unter dem Gebraucht von **Modalverben** dokumentiert. Diese Modalverben zeigen auf, welche Anforderungen in welchem Maße übernommen werden müssen. So bedeutet:

- **MUSS / DARF NUR**, dass diese Anforderung obligatorisch ist und somit zwingend übernommen werden muss.
- **DARF NICHT / DARF KEIN** bedeutet, dass etwas uneingeschränkt verboten ist.
- **SOLLTE** zeigt eine Anforderung auf, welche im Normalfall erfüllt wird, jedoch nicht verpflichtend ist.

- **SOLLTE NICHT / SOLLTE KEIN** bedeutet, dass etwas normalerweise nicht getan wird, jedoch getan werden kann

(vgl. [BUN23b], IT-Grundschutz – Basis für Informationssicherheit , S. 5f).

Zusätzlich gibt es zu einer Vielzahl von Bausteinen konkrete Umsetzungshinweise [2]. Durch die Implementierung des IT-Grundschutzes können Unternehmen ihre IT-Infrastruktur effektiv schützen. Auch das Vertrauen der Kunden und Partner kann mit der Implementierung gestärkt werden, da nachgewiesen wird, dass sich aktiv und kontinuierlich mit der Informationssicherheit innerhalb des Unternehmens auseinandergesetzt wird und Maßnahmen getroffen werden.

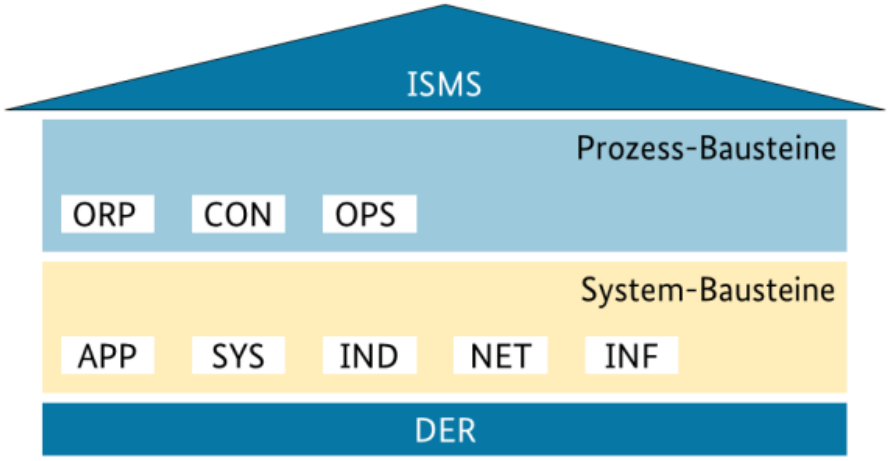

Abbildung 3.5: IT-Grundschutz-Kompendium Übersicht (vgl. [BUN23b], „Schichtenmodell und Modellierung“ S.1)

3.3 Cloud Computer Compliance Criteria Catalogue

Der **Cloud Computer Compliance Criteria Catalogue (C5)** wurde erstmalig 2016 vom BSI veröffentlicht. Die aktuelle Version stellt der C5:2020 dar (vgl. [BUN20a]). Der C5 unterstützt hierbei die Cyber-Sicherheit in dem Cloud-Computing und spezifiziert Mindestanforderungen zum sicheren Umgang mit diesem (vgl. [BUN20a], S.1). Adressiert werden hierbei hauptsächlich professionelle Cloud-Anbieter, jedoch lassen sich auch zunehmend KMU mit diesem Standard zertifizieren [3]. Vor dem Hintergrund, dass aus Kundensicht ein zertifizierter Cloud-Anbieter vertrauenswürdiger erscheint, als ein nicht zertifizierter Cloud-Anbieter, ist dieser Umstand nicht überraschend.

[2] IT-Grundschutz-Kompendium – Werkzeug für Informationssicherheit. (o.D.). - https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium$_n$ode.html[Zugriff: 10.06.2024]

[3] BSI: Kriterienkatalog Cloud Computing C5 (o.D.). - https://www.bsi.bund.de/dok/7685384[Zugriff: 11.06.2024]

Als Kriterienkatalog gliedert der C5 seine Kriterien in 17 Teilbereiche (siehe Tab. 3.1), samt Zielsetzung. Die anfallenden Kriterien werden weiterhin in Basis- und Zusatzkriterien untergliedert. **Basiskriterien** stellen das grundlegende Informationssicherheitsniveau wider, welches ein Cloud-Anbieter mit normalem Schutzbedarf innehaben sollte. Ferner können bei erhöhtem Schutzbedarf **Zusatzkriterien** herangezogen werden, um dem erhöhten Schutzbedarf Genüge zu tun. Weiterhin werden in Kapitel fünf ebenfalls Hinweise zur kontinuierlichen Prüfung und korrespondierende Kriterien für Kunden behandelt (vgl. [BUN20a], S.15f).

Bei genauerer Betrachtung bzw. Gegenüberstellung des C5 mit der ISO/IEC27001 ist festzustellen, dass diverse Bereiche in beiden Werken gleichermaßen angesprochen werden. Dies ist darauf zurückzuführen, dass der C5 auf einer breiten Auswahl an internationalen und nationalen Standards und Publikationen fußt, wie z.B. ISO/IEC27001, ISO/IEC27002 und BSI IT-Grundschutz-Kompendium. Der Detaillierungsgrad ist jedoch meist, zum Zwecke der Transparenz und Verständnis, höher als in der Orginalquelle (vgl. [BUN20a], S.18).

Nr.	Bereich	Zielsetzung
1	Organisation der Informationssicherheit (OIS)	Planung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung eines Rahmenwerks zur Informationssicherheit innerhalb der Organisation.
2	Sicherheitsrichtlinien und Arbeitsanweisungen (SP)	Bereitstellen von Richtlinien und Anweisungen bzgl. des Sicherheitsanspruchs und zur Unterstützung der geschäftlichen Anforderungen.
3	Personal (HR)	Sicherstellen, dass Mitarbeiter ihre Aufgaben verstehen, sich ihrer Verantwortung in Bezug auf Informationssicherheit bewusst sind und die Assets der Organisation bei Änderung der Aufgaben oder Beendigung geschützt werden.
4	Asset Management (AM)	Identifizieren der organisationseigenen Assets gewährleisten und ein angemessenes Schutzniveau über deren gesamten Lebenszyklus sicherstellen.
5	Physische Sicherheit (PS)	Verhindern von unberechtigtem physischem Zutritt und Schutz vor Diebstahl, Schaden, Verlust und Ausfall des Betriebs.
6	Regelbetrieb (OPS)	Sicherstellen eines ordnungsgemäßen Regelbetriebs, einschließlich angemessener Maßnahmen für Planung und Überwachung der Kapazität, Schutz vor Schadprogrammen, Protokollierung und Überwachung von Ereignissen sowie den Umgang mit Schwachstellen, Störungen und Fehlern.

Nr.	Bereich	Zielsetzung
7	Identitäts- und Berechtigungsmanagement	Absichern der Autorisierung und Authentifizierung von Benutzern des Cloud-Anbieters (in der Regel privilegierte Benutzer) zur Verhinderung von unberechtigten Zugriffen.
8	Kryptographie und Schlüsselmanagement (CRY)	Sicherstellen eines angemessenen und wirksamen Gebrauchs von Kryptographie zum Schutz der Vertraulichkeit, Authentizität oder Integrität von Information.
9	Kommunikationssicherheit (COS)	Sicherstellen des Schutzes von Informationen in Netzen und den entsprechenden informationsverarbeitenden Systemen.
10	Portabilität und Interoperabilität (PI)	Ermöglichen der Eigenschaft, den Cloud-Dienst über andere Cloud-Dienste oder IT-Systemen der Cloud-Kunden ansprechen zu können, die gespeicherten Daten bei Beendigung des Auftragsverhältnisses zu beziehen und beim Cloud-Anbieter sicher zu löschen.
11	Beschaffung, Entwicklung und Änderung von Informationssystemen (DEV)	Sicherstellen der Informationssicherheit im Entwicklungszyklus von Systemkomponenten des Cloud-Dienstes.
12	Steuerung und Überwachung von Dienstleistern und Lieferanten (SSO)	Sicherstellen des Schutzes von Informationen, auf die Dienstleister bzw. Lieferanten des Cloud-Anbieters (Subdienstleister) zugreifen können, sowie Überwachung der vereinbarten Leistungen und Sicherheitsanforderungen.
13	Umgang mit Sicherheitsvorfällen (SIM)	Gewährleisten eines konsistenten und umfassenden Vorgehens zur Erfassung, Bewertung, Kommunikation und Behandlung von Sicherheitsvorfällen.
14	Kontinuität des Geschäftsbetriebs und Notfallmanagement (BCM)	Planen, Implementieren, Aufrechterhalten und Testen von Verfahren und Maßnahmen zur Kontinuität des Geschäftsbetriebs und für das Notfallmanagement.
15	Compliance (COM)	Vermeiden von Verstößen gegen gesetzliche, regulatorische, selbstauferlegte oder vertragliche Anforderungen zur Informationssicherheit und Überprüfen der Einhaltung.
16	Umgang mit Ermittlungsanfragen staatlicher Stellen (INQ)	Gewährleisten eines angemessenen Umgangs mit Ermittlungsanfragen staatlicher Stellen hinsichtlich juristischer Überprüfung, Information der Cloud-Kunden und Begrenzung des Zugriffs auf oder der Offenlegung von Daten.

Nr.	Bereich	Zielsetzung
17	Produktsicherheit (PSS)	Bereitstellen aktueller Informationen zur sicheren Konfiguration und über bekannte Schwachstellen des Cloud-Dienstes für Cloud-Kunden, geeigneter Mechanismen zur Fehlerbehandlung und Protokollierung sowie zur Authentisierung und Autorisierung von Benutzern der Cloud-Kunden.

Tabelle 3.1: BSI C5: 17 Bereiche des Katalogs
(Quelle: nach [BUN20a], S.15)

4 Erfüllung der gesetzlichen Anforderungen durch Normen und Standards

Das folgende Kapitel stellt den Hauptarbeitsteil dieser Arbeit dar. Es wird in den Unterkapiteln jeweils ein Gesetz bzw eine Verordnung thematisiert, indem die übereinstimmenden Maßnahmen ausgewählt werden. Hierzu wird der Gedankengang zur Auswahl dargelegt und die anfallenden Maßnahmen erläutert.

Da die vorliegende Arbeit hauptsächlich an nationale Interessensträger adressiert ist, wird bei der Auswahl der Gesetze bzw. Verordnungen, für den fertigen Katalog, stets die nationale Umsetzung einer EU-Verordnung gewählt. So werden konkret die CER-Richtlinie und die NIS2-Richtlinie nicht behandelt. Stattdessen wird für die CER-Richtlinie das KRITIS-DachG und für die NIS2-Verordnung das NIS2UmsuCG herangezogen. Dies dient dem Zweck Überschneidungen in dem Katalog zu minimieren.

4.1 CRA Konformität

Wie aus Kapitel 2.1.1 hervorgeht, stellt der CRA einen essentiellen Teil der zukünftigen Sicherheitsstrategie der Europäischen Union dar. Dabei fokussiert CRA vorwiegend die Produktsicherheit von Produkten mit digitalen Elementen. Diese Anforderungen fallen überwiegend für Hersteller solcher Produkte an. Mit der Annahme, dass KMU primär keine Hersteller, sondern Einführer oder Händler sind, werden diese Anforderungen nicht berücksichtigt. Es bleiben entsprechend die anfallenden Compliance-Anforderungen für Einführer und Händler. Diese werden thematisiert, indem sie mit den in Kapitel 3 ausgewählten Standards und Normen in Relation gebracht werden.

Zu CRA.1.1
Um diese Anforderung zu erfüllen, müssen primär vier Controls herangezogen werden. Zunächst fordert die Control A5.31 „Juristische, gesetzliche, regulatorische und vertragliche Anforderungen“, dass unter anderem auch rechtliche Anforderungen, im Bereich der Informationssicherheit, erfasst, dokumentiert und aktuell gehalten werden (vgl. [DEU24b], 5.31). In Verbindung mit A5.36 „Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit“, welche die Umsetzung der erfassten Anforderungen fordert, ist die Kontrolle der Konformität zu den jeweiligen Anhängen gegeben (vgl. [DEU24b], 5.31). Für die Meldung an den Hersteller kann die Control A5.19 „Informationssicherheit in Lieferantenbeziehungen“ in Frage kommen. Diese behandelt die Schaffung von Leitlinien in Lieferantenbeziehungen (vgl. [DEU24b], 5.19). Somit kann diese Control zur Konformität beitragen, sofern ein Meldeweg zum Hersteller geschaffen wird und in dieser Lieferantenbeziehung verankert wird. Für den Kontakt mit der Marktaufsichtsbehörde kann Control A5.5 „Kontakt mit

Behörden“ verwendet werden, welche im Kern dem Zweck der Meldung von Informationssicherheitsvorfällen an die zuständigen Behörden behandelt (vgl. [DEU24b], 5.5).
Aufgrund der gesetzlichen Definition des „*inverkehrbringen*“([EURb], Art. 3 Satz 22), können im Rahmen des IT-Grundschutz-Kompendiums nur schwer Maßnahmen angewandt werden, da dieser sich primär mit dem Betrieb von IKT-Systemen und nicht mit dem Bezug und der Bereitstellung des Produktes auf dem Handelsmarkt beschäftigt. Im weitesten Sinne kann der Baustein ORP.5 „Compliance Management“, welcher sich mit rechtlichen Anforderungen beschäftigt, angewendet werden. Die Anforderung ORP.5.A1 „Identifikation der Rahmenbedingungen“ schreibt hierzu vor, dass alle rechtlichen Anforderungen erfasst werden müssen (vgl. [BUN23b], ORP.5.A1). Nach Dokumentation der zutreffenden rechtlichen Anforderungen stellt die Berücksichtigung von OPR.5.A2 „Beachtung der Rahmenbedingungen“ sicher, dass eine Meldung an Hersteller und Marktaufsichtsbehörde erfolgt (vgl. [BUN23b], ORP.5.A2). Etwaige Baustein-Anforderungen, wie z.B. DER.2.1.A4 „Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen“, welche Meldepflichten im Bezug auf Behörden mit einschließt, können in diesem Fall keine Anwendung finden, da diese Anforderung erst nach Eintreten des Sicherheitsvorfalls greift und somit für den vorliegenden Fall keine Relevanz besitzt (vgl. [BUN23b], DER.2.1.A4).
Aufseiten des C5-Katalogs erfolgt die Ermittlung und Dokumentation der rechtlichen Anforderungen an den Cloud-Dienst durch COM-01 „Identifizierung anwendbarer gesetzlicher, regulatorische, selbstauferlegter oder vertraglicher Anforderungen“ (vgl. [BUN20a], COM-01). Die Einhaltung der dokumentierten Anforderungen wird durch Kriterium COM-03 „Interne Audits des Informationssicherheitsmanagementsystems“ sichergestellt, indem diese zu regelmäßigen, jedoch mind. jährlichen, internen Audits verpflichtet (vgl. [BUN20a], COM-03). Darüber hinaus kann SSO-04 „Überwachung der Einhaltung der Anforderungen“ angewendet werden. SSO-04 stellt die Überprüfung der Einhaltung, in Hinblick auf die gesetzlichen Anforderungen, sicher (vgl. [BUN20a], SSO-04). Zum Zwecke der Meldung an die Marktaufsichtsbehörde und Hersteller könnte Kriterium OIS-05 „Kontakt zu relevanten Behörden und Interessensverbänden“ Anwendung finden. Es ist fraglich, ob dies exakt der Fall ist, da das Kriterium den Kontakt einseitig in Richtung des Cloud-Anbieters beschreibt und keinen beidseitigen Informationsfluss beschreibt (vgl. [BUN20a], OIS-05).

Zu CRA.1.2

Eine Organisation kann durch die Berücksichtigung der Control A5.19 „Informationssicherheit in Lieferantenbeziehungen“ eine Konformität mit CRA.1.2 erlangen. Diese Control ist anwendbar, da das gesetzlich geforderte Konformitätsverfahren unter anderem die Einhaltung der Anforderungen an die Cybersicherheit aus Anhang 1 fordert und somit die, für die Control relevante, Informationssicherheit anspricht (vgl. [DEU24b], 5.19). Zur Konformität mit CRA.1.2 ist jedoch zu beachten, dass dies nur gegeben ist, wenn bei Umsetzung ein festes Verfahren, zur Überprüfung dieser Kriterien, etabliert und umgesetzt wird.
Erneut kann aufgrund der gesetzlichen Definition des „*inverkehrbringen*“ ([EURb], Art. 3 Satz 22), im Rahmen des IT-Grundschutz-Kompendiums, nur schwer Maßnahmen ausgemacht werden, da dieses sich primär mit dem Betrieb von IKT-Systemen beschäftigt und nicht mit dem Bezug und

Weiterverkauf. Da es sich jedoch erneut um eine rechtliche Anforderung handelt, findet ORP.5 „Compliance Management“ erneut Anwendung. Ebenfalls ORP.5.A1 „Identifikation der Rahmenbedingungen“ und ORP.5.A2 „Beachtung der Rahmenbedingungen“ können, wie zuvor bei CRA.1.1, Anwendung finden.
Im Rahmen des C5-Kriterienkatalogs könnte SP-01 „Dokumentation, Kommunikation und Bereitstellung von Richtlinien und Anweisungen“ Anwendung finden. Eines der Basiskriterien hierbei ist die Dokumentation und Kommunikation von anwendbaren rechtlichen Anforderungen (vgl. [BUN20a], SP-01). In Verbindung mit COM-03 „Interne Audits des Informationssicherheitsmanagementsystems“, könnte man eine Konformität erreichen, da COM-03 durch interne Audits sicherstellt, dass die dokumentierten Anforderungen umgesetzt und eingehalten werden (vgl. [BUN20a], COM-03).

Zu CRA.1.3

Zu dieser Anforderung konnte in der ISO 27001 keine konkrete Control ausgemacht werden. Spekulativ könnte man davon ausgehen, dass A5.31 „Juristische, gesetzliche, regulatorische und vertragliche Anforderungen“ herangezogen werden kann. Wie bereits in den vorangegangenen Anforderungen erwähnt, fordert diese Control, dass die anwendbaren gesetzlichen Anforderungen dokumentiert werden (vgl. [DEU24b], 5.31). In Folge wird sichergestellt, dass diese dokumentierten gesetzlichen Anforderungen durch A5.36 „Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit“ eingehalten werden (vgl. [DEU24b], 5.36).
Der Baustein ORP.5 „Compliance Management“ beschäftigt sich mit rechtlichen Anforderungen. Die Anforderung ORP.5.A1 „Identifikation der Rahmenbedingungen“ schreibt hierzu vor, dass alle rechtlichen Anforderungen erfasst werden müssen (vgl. [BUN23b], ORP.5.A1). Nach Dokumentation der zutreffenden rechtlichen Anforderungen stellt die Berücksichtigung von OPR.5.A2 „Beachtung der Rahmenbedingungen“ sicher, dass die entsprechenden Informationen dem Produkt beigefügt werden (vgl. [BUN23b], ORP.5.A2).
Aufseiten des C5-Katalogs lässt sich eventuell BC-01 „Angaben zu Gerichtsbarkeit und Lokation“ anwenden. Durch diese wird der Cloud-Anbieter dazu verpflichtet innerhalb der Vertragsvereinbarung und Systembeschreibung Angaben zur Lokation und Gerichtsbarkeit zu machen, jedoch beschreiben die weiteren Ausführungen, dass der Umfang der Angaben sich an dem durch den Auftraggeber vorgegebenen Maß orientiert (vgl. [BUN20a], BC-01). Wenn der Auftraggeber vom Cloud-Anbieter also fordert, dass die gesetzlich geforderten Angaben gemacht werden, könnte BC-01 die Erfüllung von CRA.1.3 abdecken.

Zu CRA.1.4

Die ISO 27001 verfügt zur Konformität von CRA.1.4 vier Controls, welche in Kombination angewendet werden sollten. Zunächst sorgt Control A5.31 „Juristische, gesetzliche, regulatorische und vertragliche Anforderungen“ dafür, dass die rechtlichen Konformitätsbestimmungen erfasst werden und in die produktspezifische Richtlinie aufgenommen wird (vgl. [DEU24b], 5.31). A5.36 „Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit“ sorgt für die Überwachung dieser Richtlinie und fordert eine stetige Risikobeurteilung, wobei bei Nichtkonformität ggf. Korrek-

turmaßnahmen getroffen werden (vgl. [DEU24b], 5.36). Für die Meldung an den Hersteller kann Control A5.6 „Kontakt mit speziellen Interessensgruppen“ herangezogen werden. Der Hersteller wird hierbei zwar nicht als ein sicherheitsorientierter Fachverband oder Expertenforum betrachtet, jedoch lässt die Formulierung der *speziellen Interessensgruppen* den nötigen Interpretationsraum, um den Hersteller als dies zu sehen (vgl. [DEU24b], 5.6). Für den Kontakt mit der Marktaufsichtsbehörde kann Control A5.5 „Kontakt mit Behörden“ verwendet werden, welche exakt mit dem Meldungskriterium übereinstimmt (vgl. [DEU24b], 5.5).
Zur Erfüllung der geforderten Korrekturmaßnahmen, durch das IT-Grundschutz-Kompendium, lässt sich ORP.5.A2 „Einhaltung der Rahmenbedingungen“ anwenden. Grundlage hierbei sind die zuvor, über ORP.5.A1 „Identifikation der Rahmenbedingungen“, erfassten Rahmenbedingungen. Konkret schreibt ORP.5.A2 den Einsatz von sachgerechten Korrekturmaßnahmen vor, was zu einer Übereinstimmung mit der gesetzlichen Anforderung führt (vgl. [BUN23b], ORP.5.A2). Die entsprechende Meldung an die Marktaufsichtsbehörde könnte auf Grundlage von DER.2.1.A4 „Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen“ erfolgen, welche eine Mitteilung an die entsprechende Behörde fordert (vgl. [BUN23b], DER.2.1.A4). *Könnte* wird hierbei gewählt, da das bloße Vorhandensein eines Cybersicherheitsrisikos noch keinen Vorfall darstellt und somit streng genommen noch nicht durch DER.2.1.A4 zu einer Meldung führt.
Aufseiten des C5-Katalogs erfolgt die Ermittlung und Dokumentation der rechtlichen Anforderungen an den Cloud-Dienst durch COM-01 „Identifizierung anwendbarer gesetzlicher, regulatorische, selbstauferlegter oder vertraglicher Anforderungen“ (vgl. [BUN20a], COM-01). Die Einhaltung der dokumentierten Anforderungen wird durch Kriterium COM-03 „Interne Audits des Informationssicherheitsmanagementsystems“ sichergestellt, indem dies zu regelmäßigen, jedoch mind. jährlichen, internen Audits verpflichtet (vgl. [BUN20a], COM-03). Darüber hinaus kann SSO-04 „Überwachung der Einhaltung der Anforderungen“ angewendet werden. SSO-04 stellt die Überprüfung in Hinblick auf die gesetzlichen Anforderungen sicher (vgl. [BUN20a], SSO-04). Zum Zwecke der Meldung an die Marktaufsichtsbehörde und Hersteller könnte Kriterium OIS-05 „Kontakt zu relevanten Behörden und Interessensverbänden“ Anwendung finden. Es ist fraglich, ob dies exakt der Fall ist, da das Kriterium den Kontakt einseitig in Richtung des Cloud-Anbieters beschreibt und keinen beidseitigen Informationsfluss beschreibt (vgl. [BUN20a], OIS-05).

Zu CRA.1.5

Zur Erfüllung von CRA.1.5 können zwei Controls der ISO 27001 angewendet werden. Zum einen fordert Control A5.33 „Schutz von Aufzeichnungen“, dass die rechtlichen Anforderungen an Aufzeichnungen erfasst, dokumentiert und eingehalten werden und, dass eine sichere Verwahrung stattfindet (vgl. [DEU24b], 5.33). Zum Zwecke der Übermittlung an die Marktaufsichtsbehörde lässt sich in Maßen A5.5 „Kontakt mit Behörden“ anwenden. Zwar ist diese vorwiegend auf die Meldung von Informationssicherheitsvorfällen ausgelegt, jedoch wird auch ein allgemeiner Informationsfluss angesprochen, worunter eine solche Übermittlung fallen sollte (vgl. [DEU24b], 5.5).
Das IT-Grundschutz-Kompendium behandelt die Aufbewahrung von Dokumenten, oder auch Archivierung, im gleichnamigen Baustein OPS.1.2.2 „Archivierung“. Hierbei wird anhand von 22

Anforderungen sichergestellt, dass sämtlich Dokumente, gemäß ihren Anforderungen, archiviert und verfügbar sind (vgl. [BUN23b], OPS.1.2.2). Zum Zweck des Vorzeigens des Konformitätsnachweises konnte keine konkrete Anforderung im IT-Grundschutz-Kompendium ausgemacht werden.
Im Rahmen des C5-Katalogs konnte lediglich COM-01 „Identifizierung anwendbarer gesetzlicher, regulatorische, selbstauferlegter oder vertraglicher Anforderungen“ als beitragend, zu der Erfüllung von CRA.1.6, ausgemacht werden. Hierbei wird die Definition und Dokumentationen von relevanten gesetzlichen Anforderungen und damit einhergehende Verfahren zur Einhaltung, gefordert (vgl. [BUN20a], COM-01). Ein Kriterium zur Nachweiserbringung des Konformitätsnachweises konnte nicht gefunden werden.

Zu CRA.1.6

Zur Erfüllung dieser Anforderung kann erneut die Control A5.5 „Kontakt mit Behörden“ verwendet werden. Zwar ist diese vorwiegend auf die Meldung von Informationssicherheitsvorfällen ausgelegt, jedoch wird auch ein allgemeiner Informationsfluss angesprochen, worunter eine solche Meldung fallen sollte (vgl. [DEU24b], 5.5).
Im weitesten Sinne kann der Baustein ORP.5 „Compliance Management“, welcher sich mit rechtlichen Anforderungen beschäftigt, angewendet werden. Die Anforderung ORP.5.A1 „Identifikation der Rahmenbedingungen“ schreibt hierzu vor, dass alle rechtlichen Anforderungen erfasst werden müssen (vgl. [BUN23b], ORP.5.A1). Nach Dokumentation der zutreffenden rechtlichen Anforderungen stellt die Berücksichtigung von ORP.5.A2 „Beachtung der Rahmenbedingungen“ sicher, eine entsprechende Meldung erfolgt (vgl. [BUN23b], ORP.5.A2).
Im Rahmen des C5-Katalogs kann zu CRA.1.6 lediglich COM-01 „Identifizierung anwendbarer gesetzlicher, regulatorische, selbstauferlegter oder vertraglicher Anforderungen“ angewendet werden, da es sich hierbei um eine gesetzliche Anforderung handelt und der Cloud-Anbieter somit durch COM-01 verpflichtet wird diese zu erfassen (vgl. [BUN20a], COM-01). Darüber hinaus verfügt der C5-Katalog über keine weiteren Kriterien zu CRA.1.6.

Zu CRA.2.X

Bei CRA.2.1 bis CRA.2.4 findet eine Verschiebung nach hinten innerhalb der Lieferkette statt. Entsprechend werden lediglich Anforderungen gestellt, welche bereits unter CRA.1.X erläutert wurden. An dieser Stelle werden etwaige Erläuterungen ausgelassen und es wird auf die passenden Erläuterungen CRA.1.X verwiesen.

4.2 DORA Konformität

Angesichts des steigenden Bedrohungspotentials hat die Europäische Union DORA (vgl. 2.1.2) verabschiedet. DORA beinhaltet eine Vielzahl von Anforderungen, welche die Cyberresilienz adressieren. Im Folgenden wird erläutert, weshalb die angegebenen Anforderungen durch die jeweiligen

Maßnahmen erfüllt werden können.

Zu DORA.1.1

Die ISO 27001 behandelt diesen Aspekt von DORA in Control A5.1 „Informationssicherheitspolitik und -richtlinien“. Hier wird explizit in den Ausführungen in ISO 27002 erwähnt, dass die Formulierung, Veröffentlichung und Überprüfung von Informationssicherheitspolitik und themenspezifischen Richtlinien in der Verantwortung der Geschäftsleitung liegen (vgl. [DEU24b], 5.1).
Das IT-Grundschutz-Kompendium sieht die Institutionsleitung ebenfalls in der Verantwortung, eine übergeordnete Informationssicherheitsrichtlinie zu erstellen. Dies wird in der Anforderung ISMS.1.A3 „Erstellung einer Leitlinie zur Informationssicherheit“ festgelegt (vgl. [BUN23b], ISMS.1.A3).
Der C5-Katalog schließt sich dem an. Kriterium SP-01 „Dokumentation, Kommunikation und Bereitstellung von Richtlinien und Anweisungen“ zeigt zwar auf, dass die Richtlinien nicht zwangsläufig von der Institutionsleitung eingeführt werden müssen, jedoch muss jede, von der Leitlinie abgeleitete, Richtlinie von der Institutionsleitung oder dazu befugtem Personal abgesegnet werden (vgl. [BUN20a], SP-01).

Zu DORA.1.2

Zur Erfüllung dieser konkreten Anforderung konnten keine Maßnahmen in den Standards ausfindig gemacht werden.

Zu DORA.1.3

Die ISO 27001 widmet sich diesem Aspekt in den Controls A5.1 „Informationssicherheitspolitik und -richtlinien“ und A5.4 „Verantwortlichkeiten der Leitung“. Ersteres legt hierbei dar, dass die Informationssicherheitspolitik von der obersten Leitung genehmigt ist und diese Ansätze zur Erfüllung darlegt (vgl. [DEU24b], 5.1). Letzteres zeigt auf, dass die Leitung dafür zuständig ist, die Umsetzung der Maßnahmen durch das Personal sicherzustellen (vgl. [DEU24b], 5.4).
Im Rahmen des IT-Grundschutz-Kompendium legt die Anforderung ORP.5.A2 „Beachtung der Rahmenbedingungen“ fest, dass Führungskräfte für die Umsetzung der rechtlichen oder sonstigen Anforderungen zuständig sind (vgl. [BUN23b], ORP.5.A2).
Der C5-Katalog schreibt mit der Anforderung COM-03 „Interne Audits des Informationssicherheitsmanagementsystems“ vor, dass mindestens einmal jährlich die Umsetzung von gesetzlichen Maßnahmen, durch qualifiziertes Personal, kontrolliert wird (vgl. [BUN20a], COM-03). Es ist davon auszugehen, dass die Geschäftsleitung dazu qualifiziert ist und insofern wird dem geforderten „Überwachen“ Genüge getan. Der Billigunsteil wird durch SP-01 „Dokumentation, Kommunikation und Bereitstellung von Richtlinien und Anweisungen“ implizit Genüge getan, indem diese Anforderung beschreibt, dass Richtlinien und Anweisungen durch die oberste Leitung genehmigt werden (vgl. [BUN20a], SP-01).

Zu DORA.1.4

Die ISO 27001 führt zu dem Zweck der Informationssicherheitsrollen die Control A5.2 „Informa-

tionssicherheitsrollen und -verantwortlichkeiten“ an. Diese schreibt die Definition und Zuweisung von Rollen und Verantwortlichkeiten vor, welche von dem Unternehmen benötigt werden (vgl. [DEU24b], 5.2). Weiterhin werden durch die Anwendung von Control A5.19 „Informationssicherheit in Lieferantenbeziehungen“ Richtlinien und Verfahren erarbeitet, welche zu einem umfangreichen Informationssicherheitsmanagement in Lieferantenbeziehungen führen (vgl. [DEU24b], 5.19).
Das IT-Grundschutz-Kompendium behandelt diese Anforderung nicht konkret in einem Baustein bzw. mit einer spezifischen Baustein-Anforderung. Zur Erfüllung sollten primär die Baustein ISMS.1 und ORP.1 herangezogen werden. Der Baustein ISMS.1 bietet die Basis-Anforderung ISMS.1.A6 „Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit“. Diese beschreibt die Erfordernisse einer geeigneten Organisationsstruktur inklusive Rollen und Aufgaben (vgl. [BUN23b], ISMS.1.A6). Da durch DORA.1.4 eine Funktion zur Überwachung von IKT-Drittdienstleistern verpflichtend ist, so muss dies im Rahmen von ISMS.1.A6 ebenfalls integriert werden. ORP.1 verfügt ebenfalls über eine anwendbare Anforderung zur Erfüllung von DORA.1.4. Die Basis-Anforderung ORP.1.A2 „Zuweisung der Zuständigkeiten“ fordert, dass für alle Geschäftsprozesse – also auch Lieferantenmanagement – ein Sicherheitsverantwortlicher festgelegt werden muss (vgl. [BUN23b], ORP.1.A2).

Zu DORA.1.5

Die ISO 27001 behandelt die Schulung der Leitungsorganmitglieder sowohl explizit als auch implizit. Explizit wird die Schulung der Leitungsorganmitglieder in Control A6.3 „Informationssicherheitsbewusstsein, -ausbildung und -schulung“ behandelt. Diese beschreibt die Existenz eines Schulungsprogrammes zur Informationssicherheit und spricht das gesamte Personal an (vgl. [DEU24b], 6.3). Da es sich bei Mitgliedern des Leitungsorganes vorrangig ebenfalls um Personal handelt, werden diese ebenfalls angesprochen. Weiterhin ist die Leitung der Organisation durch Control A5.4 „Verantwortlichkeiten der Leitung“ dazu verpflichtet, sicherzustellen, dass die Informationssicherheitspolitik und -richtlinien adäquat durchgesetzt werden (vgl. [DEU24b],5.4). Um dieser Aufgabe nachzukommen, ist eine angemessene Kompetenz in Bezug auf Informationssicherheit eine Grundvoraussetzung, wodurch die Kenntniserlangung implizit gefordert wird.
Das IT-Grundschutz-Kompendium behandelt die Schulung von Mitarbeitern generell im Baustein ORP.3 „Sensibilisierung und Schulung zur Informationssicherheit“. Zur Erfüllung der vorliegenden Anforderung kann speziell Basis-Anforderung ORP.3.A1 „Sensibilisierung der Institutionsleitung für Informationssicherheit“ herangezogen werden. Konkret wird hier gefordert, dass die Institutionsleitung ausreichend sensibilisiert sein muss und alle Vorgesetzten mit gutem Beispiel vorangehen müssen, da diese dafür verantwortlich sind, dass die Informationssicherheitspolitik und -richtlinien umgesetzt werden (vgl. [BUN23b], ORP.3.A1). Weiterhin sollte hier die Standard-Anforderung ORP.3.A4 „Konzeption und Planung eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit“ erwähnt werden. Diese fordert ein Sensibilisierungs- und Schulungsprogramm, welches zielgruppenorientierte Schulungsmaßnahmen gewährleistet (vgl. [BUN23b], ORP.3.A1). Da es sämtliche Mitarbeiter anspricht, können hier auch, zu dem Zweck der Erfüllung von DORA.1.5, Schulungsmaßnahmen für die Institutionsleitung aufgenommen werden.

Der C5-Katalog schreibt nach Kriterium HR-03 „Programm zur Sicherheitsausbildung und Sensibilisierung“ ein „*zielgruppenorientiertes Sensibilisierungs- und Schulungsprogramm*“ (vgl. [BUN20a], HR-03) vor. Dementsprechend kann hier ebenfalls die Zielgruppe des Leitungsorgans adressiert werden und ein Programm, für dessen Mitglieder erarbeitet werden, um stets auf dem neuesten Stand der Technik in Bezug auf das gegebene Bedrohungspotenzial zu sein.

Zu DORA.1.6

Ein konkreter IKT-Risikomanagementrahmen wird durch die ISO 27001 nicht gefordert, jedoch wird die Anforderung durch mehrere Controls abgedeckt. Beginnend mit der Control A5.1 „Informationssicherheitspolitik und -richtlinien“ wird eine umfassende Reihe von Richtlinien, in Bezug auf die Informationssicherheit, gefordert. Diese müssen grundlegende Themen, wie die Definition von Informationssicherheitszielen und die fortlaufende Verbesserung des ISMS, als auch spezifische Themen, wie Kryptographie und Zugangssteuerung adressieren (vgl. [DEU24b], 5.1). Zur Schaffung eines Managementrahmens lassen sich zusätzlich Control A5.2 „Informationssicherheitsrollen und -verantwortlichkeiten“ und A5.4 „Verantwortlichkeiten der Leitung“ anwenden. Ersteres fordert die Schaffung von Aufgaben und Zuständigkeiten zur Informationssicherheit und grenzt so effektiv den Geltungsbereich des Rahmens ab (vgl. [DEU24b], 5.2). Control A5.4 weist darauf hin, dass die Leitung dafür verantwortlich ist, dass das Personal ihren Aufgaben und Zuständigkeiten nachkommt und setzt so eine Kontrolle des Personals und der Aufgaben voraus (vgl. [DEU24b], 5.4). Die Verbindung dieser drei Controls liefert das nötige Fundament für ein IKT-Risikomanagementrahmen.
Um DORA.1.6 zu erfüllen, bietet das IT-Grundschutz-Kompendium primär zwei Anforderungen aus den Bausteinen ISMS.1 und ORP.1. In dem Baustein ISMS.1 wird mit der Basis-Anforderung ISMS.1.A3 „Erstellung einer Leitlinie zur Informationssicherheit“ gefordert, dass eine übergeordnete Leitlinie zur Informationssicherheit verabschieden muss. Diese muss konkrete Sicherheitsziele und die Sicherheitsstrategie enthalten (vgl. [BUN23b], ISMS.1.A3). Weiterhin bietet der Baustein ORP.1 die Anforderung ORP.1.A1 „Festlegung von Verantwortlichkeiten und Regelungen“. Diese Basis-Anforderung verlangt, dass verbindliche Regelungen zur Informationssicherheit zu verschiedenen betrieblichen Aspekten festgelegt werden (vgl. [BUN23b], ORP.1.A1).
Der C5-Katalog fordert nach OIS-02 „Leitlinie zur Informationssicherheit“, dass die oberste Leitung eine übergeordnete Leitlinie zu verfassen hat, welche unter anderem die Sicherheitsziele der Organisation dokumentiert. Weiterhin ergeben sich durch verschiedene Kriterien weitere von der Leitlinie abgeleitete Richtlinien und Anweisungen. Namentlich OIS-06 „Richtlinie für den Umgang mit Risiken“, AM-02 „Richtlinie für den zulässigen Gebrauch und sicheren Umgang mit Assets“, PS-01 „Sicherheitsanforderungen für Räumlichkeiten und Gebäude“, PS-04 „Physische Zutrittskontrolle“, OPS-04 „Schutz vor Schadprogrammen – Konzept“, OPS-06 „Vorgaben zur Datensicherung und Wiederherstellung – Konzept“, OPS-10 „Protokollierung und Überwachung – Konzept“, OPS-11 „Protokollierung und Überwachung – Konzept zum Umgang mit Metadaten“, OPS-18 „Umgang mit Schwachstellen, Störungen und Fehlern – Konzept“, IDM-01 „Richtlinie für Zugangs- und Zugriffsberechtigungen“, CRY-01 „Richtlinie zur Nutzung von Verschlüsselungsverfahren und Schlüsselverwaltung“, COS-08 „Richtlinien zur Datenübertragung“, DEV-01 „Richtlinien

zur Entwicklung/Beschaffung von Informationssystemen“, DEV-03 „Richtlinien zur Änderung von Informationssystemen“, SSO-01 „Richtlinien und Anweisungen zur Steuerung und Überwachung Dritter“, SIM-01 „Richtlinie für den Umgang mit Sicherheitsvorfällen“, BCM-02 „Richtlinien und Verfahren zur Business Impact Analyse“, COM-02 „Richtlinie für die Planung und Durchführung von Audits“. Anhand dieser Richtlinien ist ein umfangreicher IKT-Risikomanagementrahmen gegeben (vgl. [BUN20a], OIS-02).

Zu DORA.1.7

Die Control A5.2 „Informationssicherheitsrollen und -verantwortlichkeiten“ beschäftigt sich mit der Schaffung von notwendigen Rollen und Verantwortlichkeiten, um eine effektive Verwaltung der Informationssicherheit zu gewährleisten (vgl. [DEU24b], 5.2). In Verbindung mit Control A5.3 „Aufgabentrennung“ kann sichergestellt werden, dass eine Funktion, welche für die Überwachung des IKT-Risikos zuständig ist, unabhängig ist (vgl. [DEU24b], 5.3).
Zur Erfüllung dieser Anforderungen sollten aus dem IT-Grundschutz-Kompendium primär der Baustein ISMS.1 und ORP.1 herangezogen werden. Der Baustein ISMS.1 bietet die Basis-Anforderung ISMS.1.A6 „Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit“. Diese beschreibt die Erfordernisse einer geeigneten Organisationsstruktur inklusive Rollen und Aufgaben (vgl. [BUN23b], ISMS.1.A6). ORP.1 verfügt ebenfalls über zwei anwendbare Anforderungen zur Erfüllung von DORA.1.7. Die Basis-Anforderung ORP.1.A2 „Zuweisung der Zuständigkeiten“ fordert, dass für alle Geschäftsprozesse - also auch Lieferantenmanagement – ein Sicherheitsverantwortlicher festgelegt werden muss (vgl. [BUN23b], ORP.1.A2). Um den Aspekt der „Unabhängigkeit“ zu gewährleisten, kann zusätzlich die Basis-Anforderung ORP.1.A4 „Funktionstrennung zwischen unvereinbaren Aufgaben“ aufgegriffen werden. Diese fordert, dass eine Rollen- und Funktionstrennung vorliegen muss, damit eine Person mit mehreren Rollen nicht zwischen einer der Rollen entscheiden muss und so unabhängig agieren kann (vgl. [BUN23b], ORP.1.A4).
Der C5-Katalog selber adressiert kein Kriterium zur Schaffung von bestimmten Verantwortlichkeiten und Informationssicherheitsrollen, jedoch fordert Kriterium OIS-01 „Informationssicherheitsmanagement (ISMS)“, dass der Cloud-Anbieter ein ISMS nach der ISO/IEC 27001 betreibt (vgl. [BUN20a], OIS-01). Da die ISO 27001 fordert, dass jene Verantwortlichkeiten und Rollen zur Verwaltung des ISMS definiert und dokumentiert sind (vgl. [DEU24a], A.5.2), bestehen diese Rollen auch ohne dediziertes Kriterium diesbezüglich. Darüber hinaus stellt Kriterium OIS-04 „Aufgabentrennung“ sicher, dass miteinander im Konflikt stehende Verantwortlichkeiten nicht von derselben Person ausgeübt werden (vgl. [BUN20a], OIS-04).

Zu DORA.1.8

Um diese Anforderung zu erfüllen, müssen primär zwei Controls herangezogen werden. Zunächst fordert die Control A5.31 „Juristische, gesetzliche, regulatorische und vertragliche Anforderungen“, dass unter anderem. auch rechtliche Anforderungen, im Bereich der Informationssicherheit, erfasst und erfüllt werden (vgl. [DEU24b], 5.31). Control A5.35 „Unabhängige Überprüfung der Informationssicherheit“ schreibt eine regelmäßige Prüfung der getroffenen Maßnahmen zur Informationssicherheit

vor (vgl. [DEU24b], 5.35). Der Terminus „regelmäßig“ ist hierbei nicht näher definiert, jedoch kann zu diesem Zweck die erfasste jährlich geforderte Prüfung aus Anwendung der Control A5.31 herangezogen werden.
Zum Zwecke zur Erfüllung von DORA.1.8 bietet das IT-Grundschutz-Kompendium mehrere Bausteine. Beginnen mit dem Baustein ISMS.1, wird in der Standard-Anforderung ISMS.1.A11 „Aufrechterhaltung der Informationssicherheit“ gefordert, dass die Organisationsstruktur für Informationssicherheit regelmäßig einer Revision zu unterziehen ist (vgl. [BUN23b], ISMS.1.A11). Der Baustein DER.3.1 „Audits und Revisionen“ bietet hierzu einen vertiefenden Einblick. Um die vorliegende gesetzliche Anforderung zu erfüllen, können Baustein-Anforderungen zum Thema der Revision herangezogen werden. Der Revisionsprozess wird dabei über die Vorbereitung einer Revision (vgl. [BUN23b], DER.3.1.A2), der Durchführung (DER.3.1.A4) inklusive von Dokumentenprüfungen (vgl. [BUN23b], DER.3.1.A13), der Dokumentation (vgl. [BUN23b], DER.3.1.A23), dem Abschluss (vgl. [BUN23b], DER.3.1.A24) bis hin zur Nachbereitung (vgl. [BUN23b], DER.3.1.A25) dargelegt. Grundlegend hierfür ist jedoch die Integration des Prozesses in den Informationssicherheitsprozess, welche sicherstellt eine regelmäßige Überprüfung und Verbesserung zu gewährleisten (vgl. [BUN23b], DER.3.1.A5).
Der C5-Katalog adressiert Audits und Revisionen in mehreren Kriterien. Beginnend mit der Reihe COM „Compliance“, welche dazu dient die gegebenen Anforderungen (gesetzlich, regulatorisch, selbstauferlegt, vertraglich) auf ihre Umsetzung zu kontrollieren. COM-02 „Richtlinie für die Planung und Durchführung von Audits“ fordert hierbei die Erstellung von generellen Verfahren und Anweisungen zum Thema von Audits und Revisionen (vgl. [BUN20a], COM-02). COM-03 „Interne Audits des Informationssicherheitsmanagementsystems“ fordert eine mind. jährliche Revision bzw. Auditierung des ISMS, um sicherzustellen, dass die eingangs erwähnten Anforderungen umgesetzt werden (vgl. [BUN20a], COM-03). COM-04 „Informationen über die Informationssicherheitsleistung und Managementbewertung des ISMS“ beschäftigt sich mit der Managementbewertung nach [DEU24a] Abschnitt 9.3 (vgl. [BUN20a], COM-04). Weiterhin fordert SP-02 „Überprüfung und Freigabe von Richtlinien und Anweisungen“, dass die unter DORA.1.6 (vgl. 4.2) angegebenen Richtlinien und Anweisungen mindestens jährlich auf ihre Angemessenheit überprüft werden (vgl. [BUN20a], SP-02).

Zu DORA.1.9

Zu dieser Anforderung konnten in keinem der drei Normenwerke/Standards konkrete Maßnahmen ausgemacht werden, da die Gesamtheit aller Maßnahmen eine Strategie für die digitale operationale Resilienz darstellt.

Zu DORA.1.10

Die ISO 27001 widmet sich der Verbesserung nach Informationssicherheitsvorfällen in Control A5.27 „Erkenntnisse aus Informationssicherheitsvorfällen“. Hierbei wird gefordert, dass sich die gewonnenen Erkenntnisse zunutze gemacht werden und als Grundlage für die Verbesserung der getroffenen Informationssicherheitsmaßnahmen genutzt werden (vgl. [DEU24b], 5.27).
Zum Zwecke der Nutzung von Erkenntnissen aus Informationssicherheitsvorfällen bietet das IT-Grundschutz-Kompendium zwei Anforderungen aus dem Baustein DER.2.1 „Behandlung von Sicher-

heitsvorfällen“. Die Standard-Anforderung DER.2.1.A17 „Nachbereitung von Sicherheitsvorfällen“ beschäftigt sich damit, Sicherheitsvorfälle standardisiert nachzubereiten. Hauptaugenmerk wird dabei darauf gelegt, wie schnell ein Vorfall erkannt und behoben wurde, wie effizient die internen Meldewege sind und ob die getroffenen Maßnahmen effizient waren (vgl. [BUN23b], DER.2.1.A17). Nach Bewertung können diese Erkenntnisse im nächsten Schritt weiterverwendet werden, um die internen Prozesse zu optimieren. Hierzu bietet die Standard-Anforderung DER.2.1.A18 „Weiterentwicklung der Prozesse durch Erkenntnisse aus Sicherheitsvorfällen und Branchenentwicklungen“ einen Ansatz. Hierbei werden bestehende Prozesse anhand der zuvor gewonnenen Erkenntnisse optimiert (vgl. [BUN23b], DER.2.1.A18).
Aufseiten des C5-Katalogs geht eine Ursachenanalyse eines Sicherheitsvorfalls aus dem Kriterium SIM-02 „Bearbeitung von Sicherheitsvorfällen“ hervor. Neben der Klassifikation und Priorisierung wird die Ursachenanalyse hier für jedes Ereignis gefordert, welches einen Sicherheitsvorfall darstellen könnte (vgl. [BUN20a], SIM-02). Die daraus resultierenden Informationen sollen dann, im Rahmen von SIM-05 „Auswertung und Lernprozess“, verwendet werden, um geeignete Schutzmaßnahmen zu identifizieren (vgl. [BUN20a], SIM-05).

Zu DORA.1.11

Mitarbeiterschulungen und -weiterbildung wird in der ISO 27001 mit der Control A6.3 „Informationssicherheitsbewusstsein, -ausbildung und -schulung“ behandelt. Dabei fordert diese Control, die Entwicklung eines Schulungsprogrammes, welches dazuführt, dass das Personal über ein angemessenes Informationssicherheitsbewusstsein verfügt (vgl. [DEU24b], 6.3).
Die Mitarbeitersensibilisierung und -schulung behandelt das IT-Grundschutz-Kompendium innerhalb des gleichnamigen Bausteins ORP.3 „Sensibilisierung und Schulung zur Informationssicherheit“. Die resultierenden Schulungen basieren hierbei auf der Standard-Anforderung ORP.3.A4 „Konzeption und Planung eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit“, welche ein zielgruppenorientiertes Sensibilisierungs- und Rahmenprogramm verlangt (vgl. [BUN23b], ORP.3.A4). Anhand dessen können im Anschluss Schulungen zu verschiedenen Aspekten durchgeführt werden.
Der C5-Katalog schreibt nach Kriterium HR-03 „Programm zur Sicherheitsausbildung und Sensibilisierung“ ein *zielgruppenorientiertes Sensibilisierungs- und Schulungsprogramm*. Hierbei ist sicherzustellen, dass jeder Mitarbeiter dieses Programm regelmäßig durchläuft, damit dieser auf dem aktuellen Stand der Technik ist (vgl. [BUN20a], HR-03).

Zu DORA.2.1

In den drei angeführten Standards/Normen werden keine konkreten Bausteine/Controls angeführt, welche beschreiben, inwiefern ein Protokoll oder System dem Stand der Technik entspricht. Generell lässt sich annehmen, dass sämtliche angewendeten Maßnahmen immer dem aktuellen Stand der Technik (minus Karenzzeit zur Aktualisierung des Standards) entsprechen. Auch die ungenaue Formulierung von DORA lässt hier keine weiteren Annahmen zu, ab wann ein System der neueste Stand der Technik ist, weshalb nicht versucht wird Maßnahmen zu ermitteln.

Zu DORA.2.2

Die Identifizierung und Klassifikation der IKT-gestützten Unternehmensfunktionen, Rollen, Verantwortlichkeiten, Informations- und IKT-Assets wird in der ISO 27001 in den Controls A5.9 „Inventar der Informationen und andere damit verbundener Werte“ und A5.12 „Klassifizierung von Informationen“ behandelt. A5.9 thematisiert hierbei die Inventarisierung aller Information und regelmäßiger Prüfung aller Informationen und damit verbundener Werte, samt Eigentümer der Werte. Der Eigentümer ist dann unter anderem dafür zuständig, dass diese angemessen klassifiziert und geschützt werden und periodische Überprüfungen durchgeführt werden (vgl. [DEU24b], 5.9). Wie die Informationen zu klassifizieren sind, wird in Control A5.12 erarbeitet. Hier soll die jeweilige Organisation ein Klassifizierungsschema erstellen, welches gezielt auf Grundlage Organisationsanforderungen, in Bezug auf die Informationssicherheit, basiert (vgl. [DEU24b], 5.9).
Generell ergeht aufseiten des IT-Grundschutzes eine Inventarisierung vorwiegend aus der im BSI-Standard 200-2 enthaltenen Strukturanalyse für den entsprechenden Informationsverbund (vgl.[BUN17b], Kap. 8.1). Darüber hinaus ergehen aus dem IT-Grundschutz-Kompendium jedoch an mehreren Stellen Teilklassifikationen von Assets. Die Anforderung ORP.1.A2 „Zuweisung der Zuständigkeiten“ impliziert bereits durch die Formulierung „*alle relevanten Aufgaben und Funktionen klar definiert und voneinander abgegrenzt sein*“ müssen, dass diese zuvor vollumfänglich zu erfassen sind (vgl. [BUN23b], ORP.1.A2). Weiterhin spricht die Anforderung ORP.1.A8 „Betriebsmittel- und Geräteverwaltung“ davon, dass alle Geräte und Betriebsmittel in geeigneten Bestandsverzeichnissen aufzuführen sind (vgl. [BUN23b], ORP.1.A8). Die Identifikation und Dokumentation aller IT-Assets wird in Anforderung OPS.1.1.1.A6 „Durchführung des IT-Asset-Managements“ gefordert (vgl. [BUN23b], ORP.1.1.1.A6). Auch wenn die angegebenen Maßnahmen nicht das konkret geforderte Klassifikationsdokument ergeben, dienen diese als solides Fundament zur Erstellung eines solchen Dokuments.
Der C5-Katalog forder direkt keine Auflistung der Rollen und Verantwortlichkeiten über ein Kriterium. Dies ist jedoch anhand von OIS-01 „Informationssicherheitsmanagementsystem (ISMS)“ gegeben, da hier die Existenz eines ISMS nach ISO 27001 gefordert wird (vgl. [BUN20a], OIS-01). Folglich muss auch die ISO 27001 Control A5.2 erfüllt werden, welche die Identifikation und Dokumentation von erforderlichen Informationssicherheitsrollen und -verantwortlichkeiten fordert (vgl. [DEU24a], A5.2). Bezüglich einer Inventarisierung von Assets bietet der C5-Katalog das Kriterium AM-01 „Inventarisierung der Assets“, welches eine automatische oder manuelle Inventarisierung verwendeter Assets fordert (vgl. [BUN20a], AM-01).

Zu DORA.2.3

Um effektiv Informationssicherheitsvorfälle vorbeugen zu können, gilt es stets die aktuelle Bedrohungslage zu kennen. Hierzu fordert DORA.2.3, dass betroffenen Organisationen kontinuierlich Informationen über IKT-Risiken einholen und bewerten.

Zu diesem Zweck hält die ISO 27001 die Control A8.8 „Handhabung von technischen Schwach-

stellen“ bereit. Entgegen des anders erhoffenden Namen widemt sich diese Control nicht nur der Handhabung nach Auftreten von Schwachstellen, sondern fordert, dass Informationen über Schwachstellen verwendeter Informationssysteme eingeholt, bewertet und im Anschluss durch Maßnahmen behoben werden (vgl. [DEU24b], 8.8).
Das IT-Grundschutz-Kompendium bietet mehrere Anforderungen, welche zur Erfüllung von DORA.2.3 beitragen können. So fordert die Anforderung DER.1.A12 „Auswertung von Informationen aus externen Quellen“, dass die Organisation sich kontinuierlich über externe Quellen Informationen über Schwachstellen einholen sollte (vgl. [BUN23b], DER.1.A12). Weiterhin verfügt der Baustein OPS.1.1.1 über vier anwendbare Anforderungen. Zunächst fordert OPS.1.1.1.A10 „Führen eines Schwachstelleninventars“, dass die Organisation ein Schwachstelleninventar führt, welches alle bekannten Schwachstellen zu verwendeten IKT-Komponenten auflistet (vgl. [BUN23b], OPS.1.1.1.A10). Weiterhin fordert OPS.1.1.1.A20 „Prüfen auf Schwachstellen“, dass regelmäßig Informationen über bekannt gewordenen Schwachstellen zu verwendeten IKT-Komponenten eingeholt werden und entsprechend dokumentiert werden, woraus sich das Schwachstelleninventar ergibt (vgl. [BUN23b], OPS.1.1.1.A20). Darüber hinaus ergehen aus den Anforderungen OPS.1.1.1.A22 „Automatisierte Tests auf Schwachstellen“ und OPS.1.1.1.A23 „Durchführung von Penetrationstests“ der automatisierte und manuelle Test auf Schwachstellen (vgl. [BUN23b], OPS.1.1.1.A20 und OPS.1.1.1.A23).
Zum Zwecke der kontinuierlichen Schwachstellenüberprüfung bietet der C5-Katalog zwei Kriterien. Zunächst fordert PSS-02 „Identifikation von Schwachstellen des Cloud-Dienstes“, dass während des Softwareentwicklungsprozesses bereits Informationen über Schwachstellen eingeholt werden (vgl. [BUN20a], PSS-02). Da dies jedoch nicht ausreicht um DORA.2.3 Genüge zu tun, kann weiterhin PSS-03 „Online-Register bekannter Schwachstellen“ herangezogen werden. Nach diesem Kriterium ist der Cloud-Anbieter dazu aufgefordert ein tagesaktuelles Online-Register von Schwachstellen zu führen oder zu verwenden, um alle Schwachstellen von verwendeten Assets zu identifizieren (vgl. [BUN20a], PSS-03).

Zu DORA.2.4

Aufseiten der ISO 27001 findet hier erneut die Control A5.9 „Inventar der Informationen und anderer damit verbundener Werte“. Diese fordert vom Eigentümer der jeweiligen Information unter anderem, dass dieser Komponenten und Interdependenzen von entsprechenden Werten auflistet (vgl. [DEU24b], 5.9).
Aufseiten des IT-Grundschutz-Kompendiums spricht die Anforderung ORP.1.A8 „Betriebsmittel- und Geräteverwaltung“ davon, dass alle Geräte und Betriebsmittel in geeigneten Bestandsverzeichnissen aufzuführen sind (vgl. [BUN23b], ORP.1.A8). Die Identifikation und Dokumentation aller IT-Assets wird in Anforderung OPS.1.1.1.A6 „Durchführung des IT-Asset-Managements“ gefordert, indem diese eine regelmäßige Prüfung der vorhandenen Assets fordert (vgl. [BUN23b], OPS.1.1.1.A6). Bezüglich einer Inventarisierung von Assets bietet der C5-Katalog das Kriterium AM-01 „Inventarisierung der Assets“, welches eine automatische oder manuelle Inventarisierung verwendeter Assets fordert. Dieses Kriterium fordert jedoch nicht, dass die entsprechenden Sicherheitskonfigurationen

ebenfalls zu dokumentieren sind (vgl. [BUN20a], AM-01). Diese werden anhand von AM-02 „Richtlinie für den zulässigen Gebrauch und sicheren Umgang mit Assets“ dokumentiert. Hier wird unter anderem die Dokumentation der *sichere Konfiguration der Mechanismen für Fehlerbehandlung, Protokollierung, Verschlüsselung, Authentisierung und Autorisierung* zu dem jeweiligen Asset gefordert (vgl. [BUN20a], AM-02).

Zu DORA.2.5

Zum Thema der Informationssicherheit in Lieferantenbeziehungen liefert die ISO 27001 die gleichnamige Control A5.19. Diese stellt generelle Richtlinien auf, welche zwingend Beachtung finden müssen (vgl. [DEU24b], 5.19). Abhängigkeiten von IKT-Drittdienstleistern werden in Control A5.21 „Umgang mit der Informationssicherheit in der IKT-Lieferkette“ thematisiert. Speziell wird hierbei gefordert, dass die entworfenen Richtlinien in der gesamten Lieferkette verbreitet werden, damit über diese ein angemessenes Sicherheitsniveau gewährleistet werden kann (vgl. [DEU24b], 5.21).
Aufseiten des IT-Grundschutz-Kompendiums greift der Baustein OPS.2.3 „Nutzung von Outsourcing“ immer dann, wenn Dienstleistungen outsourced werden. Zur Erfassung der jeweiligen Prozesse findet vor allem OPS.2.3.A1 „Erstellung von Anforderungsprofilen für Prozesse“ Anwendung, da diese Steckbriefe für diejenigen Prozesse verlangt, welche potenziell outsourced werden sollen. Diese Steckbriefe enthalten unter anderem auch Informationen über Interdependenzen zu anderen oder Subprozessen (vgl. [BUN23b], OPS.2.3.A1). In Verbindung mit Anforderung ORP.1.A1 „Festlegung von Verantwortlichkeiten und Regelungen“, welche die Abgrenzung und Dokumentation von allen relevanten Aufgaben und Funktionen fordert, kann DORA.2.5 ggf. erfüllt werden (vgl. [BUN23b], ORP.1.A1).
Das Lieferantenmanagement wird durch den C5-Katalog in der Kriterienreihe SSO „Steuerung und Überwachung von Dienstleistern und Lieferanten“ thematisiert. Hierbei sind Richtlinien und Anweisungen zur Steuerung und Überwachung Dritter zu definieren (vgl. [BUN20a], SSO-01), die Lieferanten werden einer Risikobeurteilung unterzogen (vgl. [BUN20a], SSO-02), es wird ein Verzeichnis mit diversen Identifikationsmerkmalen zu den jeweiligen Dienstleistern geführt (vgl. [BUN20a], SSO-03), es wird die Einhaltung von rechtlichen, regulatorischen und informationssicherheitstechnischen Anforderungen seitens der Lieferanten überwacht (vgl. [BUN20a], SSO-04).

Zu DORA.2.6

Die ISO 27001 fordert eine kontinuierliche Überwachung ihrer IKT-Systeme und Anwendungen innerhalb der Control A8.16 „Überwachung von Aktivitäten“. Bei Umsetzung dieser Control kann gewährleistet werden, dass anormales Verhalten erkannt und durch Korrekturmaßnahmen korrigiert werden kann (vgl. [DEU24b], 8.16).
Zum Zwecke des Monitorings bietet das IT-Grundschutz-Kompendium eine breite Auswahl an Anforderungen aus verschiedenen Bausteinen. Generelles IT-Monitoring wird durch die Anforderungen OPS.1.1.1.A9 „Durchführung von IT-Monitoring“ gefordert (vgl. [BUN23b], OPS.1.1.1.A9). Der Baustein DER.1 „Detektion von sicherheitsrelevanten Ereignissen“ fordert in Anforderung DER.1.A5 „Einsatz von mitgelieferten Systemfunktionen zur Detektion“, dass sämtliche nativ vorhandenen De-

tektionsfunktionen in IT-Systemen aktiviert sein müssen (vgl. [BUN23b], DER.1.A5). Weiterhin wird hier durch DER.1.A6 „Kontinuierliche Überwachung und Auswertung von Protokollierungsdaten“ eine möglichst permanente Überwachung von Protokollierungsdaten (vgl. [BUN23b], DER.1.A6). Darüber hinaus fordert beispielsweise DER.1.A15 „Zentrale Detektion und Echtzeitüberprüfung von Ereignismeldungen“ eine zentrale Komponente, welche Informationssichehreitsereignisse erkennt und automatisiert auswertet, sofern ein erhöhter Schutzbedarf besteht (vgl. [BUN23b], DER.1.A15). Gerade mit wachsendem Schutzbedarf wird der Einsatz von automatisierter Angriffserkennung vermehrt gefordert. So ist der Einsatz von hostbasierten Angriffserkennungssystemen auch bei Servern gefordert, wenn dieser Schutzbedarf besteht (vgl. [BUN23b], SYS.1.1.A27).
Die kontinuierliche Erkennung von Ereignissen wird von dem C5-Katalog in dem Kriterium OPS-13 „Protokollierung und Überwachung - Erkennung von Ereignissen“ behandelt. Diese fordert eine automatische Auswertung der Protokolldaten, welche zu einer Sicherheitszielverletzung führen (vgl. [BUN20a], OPS-13).

Zu DORA.2.7.1

Die Schaffung einer Informationssicherheitsleitlinie wird in der ISO 27001 in der Control A5.1 „Informationssicherheitspolitik und -richtlinien“ behandelt. Hier wird eine übergeordnete Richtlinie gefordert, welche grundlegende Sicherheitsziele definiert (vgl. [DEU24b], 5.1).
Parallel zur ISO 27001 A5.1, behandelt das IT-Grundschutz-Kompendium die Erstellung einer Leitlinie zur Informationssicherheit in der gleichnamigen Anforderung ISMS.1.A3. Hierbei wird von der Institutionsleitung verlangt eine übergeordnete Leitlinie zu verabschieden, welche Sicherheitsziele und eine Sicherheitsstrategie zur Informationssicherheit enthält (vgl. [BUN23b], ISMS.1.A3).
Der C5-Katalog verlangt dies ebenfalls anhand des Kriteriums OIS-02 „Leitlinie zur Informationssicherheit“ (vgl. [BUN20a], OIS-02).

Zu DORA.2.7.2

Bei dieser Anforderung ist die Formulierung ausschlaggebend dafür, welche Maßnahmen beachtet werden sollten. Eine *„[...] solide Struktur für Netzwerk- und Infrastrukturmanagement unter Verwendung geeigneter Techniken, Methoden und Protokolle[...]“* ([EUR23d], Art.9 (4) b)) einzurichten, kann mit der richtigen Konfiguration und Härtung von Assets gleichgesetzt werden.

Zu diesem Zweck bietet die ISO 27001 vier grundlegende Controls. Beginnend mit der Control A8.9 „Konfigurationsmanagement“ wird eine Konzipierung, Dokumentation, Umsetzung und Überwachung einer angemessenen Konfiguration von Hardware, Software und Netzwerken gefordert (vgl. [DEU24b], 8.9). Vertiefend wird vor allem das Netzwerk adressiert. Hierzu fordert Control A8.20 „Netzwerksicherheit“ die Absicherung von Netzwerken, anhand von unter anderem Klassifizierung der Informationen, Pflege der Dokumentationen, Einrichtung von Schutzmaßnahmen (vgl. [DEU24b], 8.20). Weiterhin werden in Control A8.21 „Sicherheit von Netzwerkdiensten“ Anforderungen an den Zugang zu dem jeweiligen Netzwerk gestellt (vgl. [DEU24b], 8.21) und in Control A8.22 „Trennung von Netzwerken“ in adäquate Subnetze aufgeteilt (vgl. [DEU24b], 8.22).

Das IT-Grundschutz-Kompendium fordert zum Thema einer richtigen Konfiguration innerhalb von OPS.1.1.1.A5 „Festlegen von gehärteten Standardkonfigurationen“, dass für jede Kategorie von IT-Komponenten eine gehärtete Standardkonfiguration entwickelt und umgesetzt werden muss (vgl. [BUN23b], OPS.1.1.1.A5). Selbiges wird auch anhand von NET.3.1.A1 „Sichere Grundkonfiguration eines Routers oder Switches“ gefordert. Hierbei muss zwingend sichergestellt werden, dass nur erforderliche Dienste, Protokolle und Funktionen genutzt werden (vgl. [BUN23b], NET.3.1.A1). Die übrigen Anforderungen innerhalb von NET.3.1 beleuchten noch weitere Aspekte zur Härtung von Netzwerkgeräten (vgl. [BUN23b], NET.3.1). Durch die Anwendung der angeführten Anforderungen ist sichergestellt, dass verwendete Assets gehärtet sind und somit eine Konformität mit DORA.2.7.2 sichergestellt ist.
Der C5-Katalog behandelt die Netzwerksicherheit in den COS-Kriterien (Kommunikationssicherheit). Dabei werden von technischen Maßnahmen zum Schutz vor netzbasierten Angriffe, über die Erhebung von Sicherheitsanforderungen Verbindungen innerhalb des Netzes, die Überwachung von Verbindungen zu internen und externen Netzen, Einrichtung und Unterhaltung von Netzgateways für Netzübergreifende Zugriffe, Einrichtung und Unterhaltung von gesonderten Netzen zur Administration, Segregation des Kunden-Datenverkehrs und dem Netzverkehr des Cloud-Betreibers, Dokumentation der logischen Struktur des Netzes bis hin zu Richtlinien und Anweisungen mit Schutzmaßnahmen bei der Datenübertragung thematisiert (vgl. [BUN20a], COS-01 bis COS-08).

Zu DORA.2.7.3

Die Zugangsverwaltung wird durch die ISO 27001 grundlegend in den Controls A5.15 „Zugangssteuerung“, A5.18 „Zugangsrechte“ und A8.3 „Informationszugangsbeschränkung“ geregelt. Die Control A5.15 beschäftigt sich hierbei mit einer grundlegenden Richtlinie zur Schaffung und Verwaltung von logischen und physischen Zugangsrechten (vgl. [DEU24b], 5.15). Die Control A5.18 vertieft die Überlegungen, welche zur Erteilung, Entzug und Überprüfung von Zugangsrechten führen. Die Ausführungen der ISO 27002 geben dabei 16 Aspekte zu diesen Kategorien an, sodass eine umfangreiche Beleuchtung vorgenommen werden kann (vgl. [DEU24b], 5.18). Die Control A8.3 spielt zur Erfüllung der Anforderung insofern eine Rolle, als diese die technische Umsetzung der erarbeiteten Richtlinie beleuchtet (vgl. [DEU24b], 8.3). Darüber hinaus existieren noch weitere Control, welche sich beispielsweise mit der Zugangsbeschränkung zu Quellcode beschäftigen (vgl. [DEU24a], A8.4).
Das BSI IT-Grundschutz-Kompendium hat zu diesem Themenbereich den Baustein ORP.4 „Identitäts- und Berechtigungsmanagement“. Hierbei bieten bereits die Basis-Anforderungen eine umfangreiche Beleuchtung des Zugangsmanagements. Besonders interessant zur Erfüllung von DORA.2.8.3 sind hierbei ORP.4.A2 „Einrichtung, Änderung und Entzug von Berechtigungen“, ORP.4.A5 „Vergabe von Zutrittsberechtigungen“, ORP.4.A6 „Vergabe von Zugangsberechtigungen“ und ORP.4.A7 „Vergabe von Zugriffsrechten“. ORP.4.A2 schreibt vor, dass Benutzendenkennungen und Berechtigungen nur jeweils über die für ihre Arbeit notwendigen Berechtigungen Verfügen dürfen (vgl. [BUN23b], ORP.4.A2). Darüber hinaus wird von DORA.2.8.3 eine Richtlinie gefordert, welche die Verwaltung der beschriebenen Rechte festlegt. Hierfür kann zusätzlich die Standard-Anforderung ORP.4.A16 „Richtlinien für die Zugriffs- und Zugangskontrolle“ herangezogen werden, welche beschreibt, dass

eine solche Richtlinie zur Zugriffs- und Zugangsverwaltung für jedes IT-System bzw IT-Anwendung separat vorhanden sein sollte (vgl. [BUN23b], ORP.4.A16).
Ähnlich wie das IT-Grundschutz-Kompendium bietet auch der C5-Katalog eine Vielzahl von Kriterien zum Identitäts- und Berechtigungsmanagement (IDM). Beginnend mit dem Kriterium IDM-01 „Richtlinie für Zugangs- und Zugriffsberechtigungen“ werden grundlegende Geschäfts- und Sicherheitsanforderungen und Zugangs- sowie Zugriffsberechtigungen zu automatisierten Autorisierungsprozessen ermittelt und dokumentiert (vgl. [BUN20a], IDM-01). Des Weiteren werden mithilfe von IDM-02 „Vergabe und Änderung von Zugangs- und Zugriffsberechtigungen“ Verfahren für die Vergabe von Zugangs- und Zugriffsberechtigungen festgelegt (vgl. [BUN20a], IDM-02). IDM-03 und IDM-04 liefern zwei konkrete Szenarien wann ein Entzug oder eine Sperrung von etwaigen Zugriffsberechtigungen vollzogen werden sollte (vgl. [BUN20a], IDM-02 und IDM-03). Damit die jeweiligen Berechtigungen nur den nötigen Mitarbeitern vergeben werden, werden diese durch IDM-05 „Regelmäßige Überprüfung der Zugriffsberechtigungen“ mindestens jährlich verpflichtend überprüft und ggf. angepasst (vgl. [BUN20a], IDM-05). Technisches Personal, was privilegierte Zugriffsberechtigungen benötigt, erhält diese nur nach einem Verfahren, was IDM-01 entspringt (vgl. [BUN20a], IDM-06). Damit sichergestellt ist, dass nur die jeweilig gewollten Personen die Berechtigungen nutzt, werden hinreichende Authentisierungsmaßnahmen in den Kriterien IDM-08 und IDM-09 thematisiert. Durch die Umsetzung aller aufgezeigten Kriterien sollte DORA.2.8.3 Genüge getan sein.

Zu DORA.2.7.4

Die ISO 27001 behandelt das Thema der Authentifizierung und Authentisierung vorwiegend in den Controls A5.16 „Identitätsmanagement“, A5.17 „Authentisierungsinformationen“ und A8.5 „Sichere Authentisierung“. Control A5.16 gibt dabei allgemeine Verfahren zur Identitätsverwaltung vor, während die Verwaltung der Authentisierungsinformationen behandelt (vgl. [DEU24b], 5.16). A8.5 leistet Hilfe zur technischen Implementierung von Authentisierungsverfahren, welche auf Grundlage der zuvor bestimmten Richtlinien zur Zugangssteuerung geschaffen wurden (vgl. [DEU24b], 8.5).
Zur Erfüllung dieser Anforderung wird erneut Baustein ORP.4 „Identitäts- und Berechtigungsmanagement“ verwendet. Um eine starke Authentisierung gewährleisten zu können, können die Anforderungen ORP.4.A9 „Identifikation und Authentisierung“, ORP.4.A12 „Entwicklung eines Authentisierungskonzeptes für IT-Systeme und Anwendungen“, ORP.4.A13 „Geeignete Auswahl von Authentisierungsmechanismen“, ORP.4.A18 „Einsatz eines zentralen Authentisierungsdienstes“ herangezogen werden. ORP.4.A9 schreibt vor, dass der Zugriff zu IT-Systemen generell durch Identifikation und Authentisierung des Benutzenden geschützt sein müssen. Hierzu muss jedoch ein Konzept bestehen, welches in ORP.4.A12 erarbeitet wird. Weiterhin fordert dieser Baustein explizit, dass die resultierenden kryptografischen Schlüssel durch geeignete Schutzmaßnahmen gesichert werden müssen (vgl. [BUN23b], ORP.4.A9). Somit wird dieser Teil von DORA.2.7.4 bereits abgedeckt. ORP.4.A13 beschreibt, dass die Authentisierungsdaten während des gesamten Anmeldevorgangs gesichert sein sollten (vgl. [BUN23b], ORP.4.A13). Damit die Authentisierung an allen Assets zentral überwacht werden kann, fordert ORP.4.A18 einen zentralen netzbasierten Authentisierungsdienst (vgl. [BUN23b], ORP.4.A18). Sollten der Schutzbedarf über die aufgezeigten Anforde-

rungen hinausgehen, bietet der Baustein zur Authentisierung zusätzlich die Anforderung ORP.4.A21 „Mehr-Faktor-Authentisierung“, welche den Einsatz von Mehr-Faktor-Authentisierung, anhand von kryptografischen Zertifikaten, Chipkarten oder Token beschreibt (vgl. [BUN23b], ORP.4.A21).
Authentisierungsmechanismen werden durch den C5-Katalog im gleichnamigen Kriterium IDM-09 „Authentisierungsmechanismen thematisiert. Hierbei wird ein automatisierter Authentisierungsprozess gefordert, welcher ebenfalls Zwei- oder Mehr-Faktor-Authentisierung beinhaltet, sofern die Produktionsumgebung gefragt ist. Sollte dabei zur Authentisierung ein Passwort verwendet werden, ist der Cloud-Anbieter dazu verpflichtet dieses bei serverseitiger Speicherung durch kryptografische Passworthashfunktionen zu schützen (vgl. [BUN20a], IDM-09). Bei der Verwendung von digital signierten Zertifikaten gilt es Kriterium CRY-01 zu beachten.

Zu DORA.2.7.5

Zum Zwecke des Änderungsmanagements bietet die ISO 27001 die Control A8.32 „Änderungssteuerung“. Hierbei wird vorgegeben, dass Änderungen von Informationssystemen Gegenstand von einem festen Verfahren sind und dementsprechend Regeln und formellen Prozessen unterliegen (vgl. [DEU24b], 8.32).
Ein Änderungsmanagement beleuchtet das IT-Grundschutz-Kompendium im Baustein OPS.1.1.3 „Patch- und Änderungsmanagement“. Besonders relevant sind hierbei die Anforderungen OPS.1.1.3.A1 „Konzept für das Patch- und Änderungsmanagement“, OPS.1.1.3.A5 „Umgang mit Änderungsanforderungen“, OPS.1.1.3.A6 „Abstimmung von Änderungsanforderungen“ und OPS.1.1.3.A7 „Integration des Änderungsmanagements in die Geschäftsprozesse“. OPS.1.1.3.A1 fordert hierbei das Vorhandensein eines angemessenen Änderungsmanagements, welches ebenfalls Sicherheitsaspekte berücksichtigt (vgl. [BUN23b], OPS.1.1.3.A1). Da eine Änderung im Normalfall einer Änderungsanforderung entspringt, wird der Umgang mit dieser in OPS.1.1.3.A5 behandelt. Es wird definiert, dass jede Anforderung dokumentiert werden muss und auf die Informationssicherheit durch den Fachverantwortlichen kontrolliert werden muss (vgl. [BUN23b], OPS.1.1.3.A5). Da der Fachverantwortliche jedoch nicht alleine über eine Änderung entscheiden sollte, schreibt OPS.1.1.3.A6 vor, dass sich alle relevanten Zielgruppen nachweisbar dazu äußern dürfen können (vgl. [BUN23b], OPS.1.1.3.A6). Dieser ganze Änderungsprozess sollte dabei effizient in die Geschäftsprozesse integriert werden, um Störungen durch Änderungen zu vermeiden. Hierzu bietet der Baustein die Anforderung OPS.1.1.3.A7, welche herausstellt, dass die aktuelle Situation zwingend zu berücksichtigen ist und alle betroffenen Fachabteilungen über Änderungen informiert werden sollten (vgl. [BUN23b], OPS.1.1.3.A7).
Ein risikobasiertes Änderungsmanagement wird durch den C5-Katalog in den Kriterien DEV-03 „Richtlinie zur Änderung von Informationssystemen“ und DEV-05 „Risikobewertung, Kategorisierung und Priorisierung von Änderungen“ thematisiert. DEV-03 fordert hierbei einleitend die Erarbeitung einer Richtlinie, welche grundlegende Verfahren und Anweisungen zur Verwaltung von Änderungen beinhaltet (vgl. [BUN20a], DEV-03). Die festgelegten Verfahren werden im Folgenden DEV-05 Kriterium verwendet, um die jeweiligen Assets auf potenzielle Risiken und deren Auswirkungen zu untersuchen (vgl. [BUN20a], DEV-05).

Zu DORA.2.7.6

Da einem Patchmanagement meist eine Schwachstelle und eine dementsprechende Korrekturmaßnahme unterliegt, kann zu diesem Zweck die Control A8.8 „Handhabung von technischen Schwachstellen“ herangezogen werden, da diese ein allgemeines Verfahren zur Einholung von Informationen über Schwachstellen und entsprechende Behebung durch Maßnahmen vorgibt (vgl. [DEU24b], 8.8). Weiterhin beschäftigt sich Control A8.9 „Konfigurationsmanagment“ ebenfalls mit dieser Anforderung, da zwangsläufig die getroffene Korrekturmaßnahme in die zu erstellende Sicherheitsdokumentation aufgenommen werden muss (vgl. [DEU24b], 8.9). Da bei der Patchdurchführung um eine Änderung des betroffenen Informationssystems handelt, muss zwangsläufig der Prozess zum Änderungsmanagement durchlaufen werden (vgl. [DEU24b], 8.32).
Das Patchmanagement behandelt das IT-Grundschutz-Kompendium im Baustein OPS.1.1.3. Relevant für das Patchmanagement sind hierbei die Anforderungen OPS.1.1.3.A1 „Konzept für das Patch- und Änderungsmanagement“, OPS.1.1.3.A3 „Konfiguration von Autoupdate-Mechanismen“, OPS.1.1.3.A15 „Regelmäßige Aktualisierung von IT-Systemen und Software“, OPS.1.1.3.A7 „Integration des Änderungsmanagements in die Geschäftsprozesse“ und OPS.1.1.3.A8 „Sicherer Einsatz von Werkzeugen für das Patch- und Änderungsmanagement“. OPS.1.1.3.A1 fordert hierbei das Vorhandensein eines angemessenen Änderungsmanagements, welches ebenfalls Sicherheitsaspekte berücksichtigt (vgl. [BUN23b], OPS.1.1.3.A1). Verfügt eine eingesetzte Software über einen Aktualisierungsautomatismus, schreibt OPS.1.1.3.A3 vor, dass dieser passend konfiguriert und abgesichert sein muss (vgl. [BUN23b], OPS.1.1.3.A3). OPS.1.1.3.A15 schreibt die regelmäßige Aktualisierung von Soft- und Hardware vor. Dies hat den Hintergrund, dass bei Hardware keine Hardware verwendet wird, welche vom Hersteller nicht mehr unterstützt wird und aufseiten der Software kann so sichergestellt werden, dass erkannte Schwachstellen möglichst zeitnah behoben werden können (vgl. [BUN23b], OPS.1.1.3.A15). Auch bei dem Patchmanagement muss darauf geachtet werden, dass dieses in den Geschäftsprozess integriert ist, damit der Geschäftsprozess nicht unnötig gestört wird. Hierzu wird in OPS.1.1.3.A7 gefordert, dass alle relevanten Fachabteilungen von einem Patch zu informieren sind und die aktuelle Situation (Stand des Geschäftsprozesses) berücksichtigt werden muss (vgl. [BUN23b], OPS.1.1.3.A7). Entscheidet sich eine Organisation dazu ein Patchmanagementwerkzeug zu verwenden, so sind Verfahren und Richtlinien diesbezüglich zu erstellen, welche auch eine Sicherheitsrichtlinie beinhalten (vgl. [BUN23b], OPS.1.1.3.A7).
Richtlinien in Bezug auf Patch- und Updatemanagement werden durch den C5-Katalog primär mit dem DEV-03 „Richtlinien zur Änderung von Informationssystemen“ behandelt. Diese fordert, dass der Cloud-Dienst Richtlinien und Anweisungen mit Maßnahmen zum Thema des Änderungsmanagements dokumentiert, kommuniziert und bereitstellt. Konkret werden dabei unter anderem Anforderungen an die Änderungen, Anforderungen an die Durchführung und Dokumentation von Tests und Anforderungen an die Durchführung von Notfalländerungen festgehalten (vgl. [BUN20a], DEV-03). Resultierende Änderungen werden dabei stets einer Risikobewertung, Kategorisierung und Priorisierung unterzogen (vgl. [BUN20a], DEV-05). Der C5-Katalog verpflichtet den Betreiber weiterhin, dass etwaige Software-Aktualisierungen, resultierend aus Schwachstellen, zum Kunden hin

in ihrem Online-Register bekannter Schwachstellen kommuniziert werden müssen und abgegrenzt sein muss, ob dieser den Patch selber durchzuführen hat oder der Cloud-Dienstleister den Patch durchführt (vgl. [BUN20a], PSS-03).

Zu DORA.2.8

Mechanismen zur Erkennung von Vorfällen wird in der ISO 27001 in der Control A8.16 „Überwachung von Aktivitäten“. Diese fordert, dass die Organisation ihre Netzwerke, Systeme und Anwendungen auf anormales Verhalten überwachen und ggf. Korrekturmaßnahmen ergreifen (vgl. [DEU24b], 8.16). Aufseiten des IT-Grundschutz-Kompendiums lassen sich eine Vielzahl von Anforderungen auf verschiedenen Bausteinen heranziehen. Beginnend mit OPS.1.1.1.A9 „Durchführung von IT-Monitoring“ wird eine grundsätzliche Überwachung von IKT-Assets gefordert (vgl. [BUN23b], OPS.1.1.1.A9). Weiterhin fordert DER.1.A5 „Einsatz von mitgelieferten Systemfunktionen zur Detektion“ zusätzlich, dass mitgelieferte Systemfunktionen zur Detektion, falls vorhanden, Verwendung finden müssen (vgl. [BUN23b], DER.1.A5). Da *Mechanismen* ebenfalls Personalverfahren einschließt, kann auch DER.1.A6 „Kontinuierliche Überwachung und Auswertung von Protokollierungsdaten“ Anwendung finden, welche fordert, dass ausreichende personelle Kapazitäten zur permanenten Überwachung gegeben sind (vgl. [BUN23b], DER.1.A6). Über das grundsätzliche Monitoring hinaus fordert DER.1.A9 „Einsatz zusätzlicher Detektionssysteme“, dass anhand des Netzplanes festgelegt werden soll, welche Netzsegmente durch zusätzliche Detektionssyteme geschützt werden sollte und, dass die Übergänge von internen und externen Netzen mit netzbasierten Detektionssystemen geschützt werden sollten (vgl. [BUN23b], DER.1.A9). Darüber hinaus gibt der Baustein Anforderungen an, welche auf einen erhöhten Schutzbedarf abzielen. So fordert beispielsweise DER.1.A16 „Einsatz von Detektionssystemen nach Schutzbedarfsanforderungen“ den Einsatz von automatischen Detektionssystemen, welche dem Schutzbedarf angemessen sind (vgl. [BUN23b], DER.1.A16). Ebenfalls die Anforderung SYS.1.1.A27 „Hostbasierte Angriffserkennung“ greift diesen erhöhten Schutzbedarf auf, fordert jedoch, dass es zum Einsatz von host-basierten Lösungen kommen sollte, welche das Betriebspersonal gebührend alarmieren (vgl. [BUN23b], SYS.1.1.A27). Innerhalb des C5-Katalogs wird die Erkennung von Vorfällen lediglich durch drei Kriterien thematisiert. Beginnend mit OPS-10 „Protokollierung und Überwachung - Konzept“ wird durch den Cloud-Dienst ein Konzept erarbeitet, welches Richtlinien und Anweisungen beinhaltet. Diese Richtlinien und Anweisungen stellen in erster Linie Rahmenbedingungen für die Protokollierung von Systemereignissen. Dabei werden unter anderem Sicherheitsereignisse definiert, Rollen und Verantwortlichkeiten für die Einrichtung und Überwachung der Protokollierung festgelegt oder auch die Zeitsynchronisation bei Systemkomponenten etabliert (vgl. [BUN20a], OPS-10). Auf Grundlage dieser Richtlinien werden die Protokollierungsdaten dann mit Umsetzung des Kriteriums OPS-13 „Protokollierung und Überwachung - Erkennung von Ereignissen“ automatisiert ausgewertet. Sollte eine Verletzung von Schutzzielen vorliegen, werden diese Ereignisse entsprechend an das zuständige Personal eskaliert, welche dann eine weitere Beurteilung vornimmt und Korrekturmaßnahmen einleitet (vgl. [BUN20a], OPS-13). Da hier oft dedizierte Systeme für benötigt werden und zusätzliches Personal vorhanden sein muss, wird durch die Umsetzung vom OPS-02 „Kapazitätsmanagment - Überwachung“ sichergestellt, dass ausreichend technische

Kapazitäten provisioniert werden und ausreichend Personal vorhanden ist, um schwellenwertüberschreitende Ereignisse zu handhaben (vgl. [BUN23b], OPS-02).

Zu DORA.2.9

Die ISO 27001 behandelt das Business Continuity Management (BCM) in den Controls A5.29 „Informationssicherheit bei Störungen“ und A5.30 „IKT-Bereitschaft für Business-Continuity“. A5.29 gibt hierbei vor, dass ein „angemessenes Niveau“ gewahrt werden soll (vgl. [DEU24a], A5.29). Weitere Definitionen bleiben in der Norm aus. Folglich definiert sich das angemessene Niveau aus den organisationsinternen Sicherheitszielen. Ist ein angemessenes Niveau für die Organisation definiert, sollte im nächsten Schritt überlegt werden, welche Assets im Notfall priorisiert werden sollten. Hier setzt die Control A5.30 an. Diese beschreibt einen Analyseprozess, welcher im Anschluss zu konkreten Ableitungen für IKT-Kontinuitätspläne, um eine stetige Verfügbarkeit der unternehmensinternen Informationen zu gewährleisten (vgl. [DEU24b], 5.30).
Aufseiten des IT-Grundschutz-Kompendiums wird das Thema des BCM durch den Baustein DER.4 „Notfallmanagement“ thematisiert. Grundlegend ist hierbei die Standard-Anforderung DER.4.A1 „Erstellung eines Notfallhandbuchs“, welche unter anderem die gesetzlichen geforderten Maßnahmen definiert (vgl. [BUN23b], DER.4.A1). Neben dieser elementaren Anforderung zum BCM, werden im weiteren Verlauf des Bausteins noch zusätzliche Aspekte beleuchtet, welche einem höheren Schutzbedarf entsprechen.
Der C5-Katalog bietet zum Thema des BCM eine Kriterienreihe. Angefangen mit BCM-01 „Verantwortung durch die Unternehmensleitung“ wird die oberste Leitung zum Prozessverantwortlichen des BCM ernannt und hat sicherzustellen Prozesse zu etablieren, die Umsetzung dieser zu überwachen und durch ausreichend Kapazitäten zu unterstützen (vgl. [BUN20a], BCM-01). Grundlage für das BCM stellt im C5-Katalog jedoch eine Business Impact Analyse (BIA). Die BIA stellt dabei einen sieben Schritte langen Prozess dar, welcher im Kern dazu dient herauszufinden, wie sich der Ausfall eines Prozesses auf die Unternehmung auswirkt, besonders schützenswerte Geschäftsprozesse zu ermitteln (vgl. [BUNoJ]). Richtlinien für die BIA werden hierbei durch das Kriterium BCM-02 „Richtlinien und Verfahren zur Business Impact Analyse“ definiert und dokumentiert. Nach Durchführung der BIA wird im nächsten Schritt ein Rahmenwerk zum BCM, durch Kriterium BCM-03 „Planung der Betriebskontinuität“, geschaffen. Hierbei werden unterschiedliche Aspekte, wie z.B. Zweck und Umfang der Pläne, Kommunikationswege und Rollen oder auch ein kontinuierlicher Verbesserungsprozess, berücksichtigt (vgl. [BUN20a], BCM-03). Der Cloud-Dienstleister wird dazu verpflichtet, auf Grundlage von BCM-04 „Verifizierung, Aktualisierung und Test der Betriebskontinuität“, die bestehenden Pläne und das Rahmenwerk zum BCM regelmäßig, jedoch mind. einmal jährlich auf Effektivität zu überprüfen (vgl. [BUN20a], BCM-04).

Zu DORA.2.10

Die Thematik rund um Sicherung und Wiederherstellung von Informationen wird in der ISO 27001 grundlegend in der Control A8.13 „Sicherung von Informationen“ behandelt. Dabei verlangt diese Control, dass die Organisation eine Richtlinie entwirft und regelmäßig überprüft, welche den

spezifischen Datensicherungsanforderungen gerecht wird. Es müssen also besonders gesetzlichen Anforderungen (im vorliegenden Fall DORA) erfasst werden und als Grundlage zum Entwurf der Richtlinie verwendet werden (vgl. [DEU24b], 8.13). Weiterhin fordern Absatz vier und fünf des DORA einen Aufbau von logisch und physisch redundanten Systemen. Dies wird in der ISO 27001 durch Control A8.14 „Redundanz von informationsverarbeitenden Einrichtungen“ behandelt. Konkret wird hier gefordert, dass die Organisation über ausreichend Redundanzen verfügen muss, damit die Verfügbarkeitsanforderungen erfüllt werden (vgl. [DEU24b], 8.14). Da sich die Verfügbarkeitsanforderungen hierbei erneut nach DORA richten, kann mit der Erfüllung dieser Control der gesetzlichen Anforderung Genüge getan werden.

Datensicherungskonzepte behandelt das IT-Grundschutz-Kompendium vorwiegend in dem gleichnamigen Baustein CON.3 „Datensicherungskonzept“. Hierbei wird die Erhebung von Einflussfaktoren, welche das Datensicherungskonzept essenziell beeinflussen in CON.3.A1 „Erhebung der Einflussfaktoren für Datensicherungen“ thematisiert (vgl. [BUN23b], CON.3.A1). CON.3.A2 „Festlegung der Verfahrensweisen für die Datensicherung“ fordert, dass feste Verfahren erarbeitet werden müssen, welche sich damit beschäftigen, welche Daten, wann und wie gesichert werden müssen (vgl. [BUN23b], CON.3.A2). Sind diese Verfahren erarbeitet werden in CON.3.A4 „Erstellung von Datensicherungsplänen“, die konkreten Pläne zur Datensicherung erstellt, welche spezifische Parameter des jeweiligen Systems festhält, welche das Datensicherungskonzept anwendet (vgl. [BUN23b], CON.3.A4). Um der Anforderung der regelmäßigen Tests gerecht zu werden, kann CON.3.A15 „Regelmäßiges Testen der Datensicherungen“, welche fordert, dass regelmäßig zu prüfen ist, ob die Datensicherungsverfahren wie gewünscht funktionieren (vgl. [BUN23b], CON.3.A15).
Das Thema der Datensicherung und Wiederherstellung bearbeitet der C5-Katalog primär in den Kriterien OPS-06 bis OPS-09. Im Kriterium OPS-06 „Datensicherung und Wiederherstellung - Konzept„werden generelle Richtlinien und Anweisungen zu diesem Thema festgehalten. Hierbei werden konkret Umfang, Art und Häufigkeit gemäß den vertraglichen und rechtlichen Anforderungen definiert. Weiterhin legen die Richtlinien fest, dass die Datensicherung verschlüsselt stattfinden muss und, dass der Zugriff auf die resultierenden Daten nur durch autorisierte Personen vorgenommen werden darf (vgl. [BUN20a], OPS-06). Sofern der Cloud-Dienstleister dazu vertraglich verpflichtet ist, wird dieser, durch OPS-07 „Datensicherung und Wiederherstellung - Überwachung“, zur Überwachung der Datensicherung verpflichtet. Konkret müssen technische und organisatorische Maßnahmen getroffen werden, welche verhindern, dass die Datensicherung nicht gestört wird (vgl. [BUN20a], OPS-07). Weiterhin wird der Datensicherungsprozess, auf Grundlage von OPS-08 „Datensicherung und Wiederherstellung - Regelmäßige Tests“, auf die vertraglichen Vereinbarungen hin überprüft. Sollte hier ein Defizit gegenüber den Soll-Metriken vorhanden sein, so sind diese durch qualifiziertes Personal zu beheben (vgl. [BUN20a], OPS-08). Sollen nach der Datensicherung die resultierenden Daten gespeichert (vertragliche Vereinbarung) werden, ist der Cloud-Dienstleister durch OPS-09 „Datensicherung und Wiederherstellung - Aufbewahrung“ dazu verpflichtet, die Daten zu einem Sekundärstandort zu übertragen und dort in verschlüsselter Form zu speichern (vgl. [BUN20a], OPS-09). Grundlage hierfür ist das in PS-02 „Redundanzmodell“ geforderte Redundanzmodell, was

bedeutet, dass der Betrieb des Cloud-Dienstes durch logische oder geostationäre Maßnahmen redundant erbracht wird (vgl. [BUN20a], PS-02).

Zu DORA.2.11

Die ISO 27001 befasst sich in mehreren Controls mit dem Incident Management. Angefangen bei Control A5.24 „Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen“ werden durch die Organisation Prozesse, Rollen und Verantwortlichkeiten definiert, eingeführt und kommuniziert (vgl. [DEU24b], 5.24). Durch die Schaffung eines Kommunikationskanals, im Rahmen von A6.8 „Meldung von Informationssicherheitsereignissen“ und eine offene Kommunikation dieser Meldewege, können Mitarbeiter frühzeitig einen Vorfall an die entsprechende Stelle melden (vgl. [DEU24b], 6.8). Wird ein Ereignis gemeldet, muss bestimmt werden, ob es sich hierbei um einen Informationssicherheitsvorfall handelt. Die Control A5.25 „Beurteilung und Entscheidung über Informationssicherheitsereignisse“ erarbeitet hierfür ein festes Verfahren, welches dies bestimmen soll (vgl. [DEU24b], 5.25). Wurde ein Ereignis als Informationssicherheitsvorfall eingestuft, muss eine adäquate Reaktion ausgeführt werden, um den Vorfall effektiv einzudämmen und Wiederherstellung zu leisten. Hierzu werden, im Rahmen von A5.26 „Reaktion auf Informationssicherheitsvorfälle“, Reaktionsverfahren erarbeitet und dokumentiert, welche beim Vorfallseintreten verwendet werden (vgl. [DEU24b], 5.26). Nach Vollendigung der Reaktion ist es wichtig, Beweise für eventuelle gerichtliche Verfahren zu sammeln (vgl. [DEU24b], 5.28) und auf Basis der neuen Erkenntnisse eine Verbesserung des Risikomanagementrahmens vorzunehmen (vgl. [DEU24b], 5.27). Durch die Anwendung der angeführten Controls wird ein Sicherheitsvorfall nicht nur effizient durch den Mitarbeiter gemeldet, sondern er wird auch anhand von festgelegten Verfahren behandelt und als Basis für Verbesserung genutzt.

Zum Thema der Erkennung von IKT-bezogenen Sicherheitsvorfällen, durch das IT-Grundschutz-Kompendium, wird auf die Ausführungen von DORA.2.9 verwiesen. Darüber hinaus wird aufseiten des IT-Grundschutz-Kompendiums die Behandlung und Meldung von Sicherheitsvorfällen in Baustein DER.2.1 „Behandlung von Sicherheitsvorfällen“ behandelt. Zum Thema der Meldung wird durch DER.2.1.A3 „Festlegung von Verantwortlichkeiten und Ansprechpersonen bei Sicherheitsvorfällen“ festgelegt, welcher Mitarbeiter verantwortlich ist, im Falle eines Sicherheitsvorfalles, um so ein Bewusstsein zu schaffen, an wen sich zu wenden ist. Dies ist die Grundlage für einen in DER.2.1.A9 „Festlegung von Meldewegen für Sicherheitsvorfälle“ Meldeweg, welcher im Ernstfall durch die Mitarbeitenden genutzt werden muss (DER.2.1.A4 „Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen“). Hier sollen für jede Art von Sicherheitsvorfällen ein fester Meldeweg etabliert und kommuniziert werden und wiederholt die Anforderung DER.1.A3 „Festlegung von Meldewegen“, welche im Kern das Gleiche besagt. Ist ein Sicherheitsvorfall bekannt geworden, so müssen feste Verfahren bestehen, welche sich mit der Behebung dessen beschäftigen. Diesbezüglich gilt es, als Fundament eine Richtlinie zu erstellen, welche sich hiermit beschäftigt (DER.2.1.A2 „Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen“). Der Baustein verfügt über Anforderungen, welche von der Etablierung einer Vorgehensweise zur Behebung von Sicherheitsvorfällen (DER.2.1.A7), über die Eindämmung der Auswirkungen von Sicherheitsvorfällen (DER.2.1.A10) bis

hin zur Nachbereitung von Sicherheitsvorfällen (DER.2.1.A17) reicht. Dabei werden verschiedenste Aspekte beleuchtet, um eine umfassende Strategie zur Behebung zu entwickeln.
Aufseiten des C5-Katalogs wurden die Kriterien zur Erkennung von IKT-bezogenen Vorfällen bereits im Rahmen von DORA.2.9 erläutert. Darüber hinaus etabliert der C5-Katalog den Incident Response Prozess in der SIM-Kriterienreihe. Angefangen bei SIM-01 „Richtlinie für den Umgang mit Sicherheitsvorfällen“ werden Richtlinien und Anweisungen, samt entsprechenden Maßnahmen, definiert, welche dafür sorgen, dass eine effektive und effiziente Reaktion auf Sicherheitsvorfälle gewährleistet werden kann. Bei Bekanntwerden eines Sicherheitsvorfalles ist dieser durch qualifiziertes Personal einer Klassifizierung, Priorisierung und Ursachenanalyse zu unterziehen (SIM-02 „Bearbeitung von Sicherheitsvorfällen“). Essenzieller Bestandteil des Incident Respones Prozesses, ist die Dokumentation des Vorfalles. Grundlage für die Dokumentation ist dabei die vertragliche Vereinbarung zum jeweils betroffenen Vertragskunden, welcher nach Verarbeitung des Vorfalls ebenfalls informiert werden muss (SIM-03 „Dokumentation und Berichterstattung über Sicherheitsvorfälle“). Zur Vorbeugung von ähnlichen Vorfällen wird die entstandene Dokumentation, im Rahmen von SIM-05 „Auswertung und Lernprozess“ genutzt, um Schutzmaßnahmen für zukünftige Vorfälle zu treffen.

Zu DORA.2.12

Das Klassifizieren von Informations- und Kommunikationstechnik (IKT)-bezogenen Vorfällen ist ein essenzieller Bestandteil des Incident Managements und wird in der ISO 27001 in der Control A5.25 „Beurteilung und Entscheidung über Informationssicherheitsereignisse“ behandelt. Hierfür soll ein Unternehmen ein etabliertes Schema zur Klassifizierung von Informationssicherheitsereignissen aufweisen können, damit eine effektive Reaktion auf einen eventuellen Sicherheitsvorfall gestartet werden kann.
Die Klassifizierung von Sicherheitsereignissen wird primär durch die Anforderung DER.2.1.A11 „Einstufung von Sicherheitsvorfällen“ behandelt, welche die Etablierung eines einheitlichen Verfahrens zur Einstufung von Sicherheitsvorfällen fordert.
Aufseiten des C5-Katalogs wird die Klassifizierung im Rahmen von SIM-02 „Bearbeitung von Sicherheitsvorfällen“ durchgeführt. Hierbei klassifiziert qualifiziertes Personal die jeweiligen Vorfälle anhand der in SIM-01 „Richtlinien für den Umgang mit Sicherheitsvorfällen“ definierten Vorgaben.

Zu DORA.2.13

Die externe Meldung von Informationssicherheitsereignissen wird innerhalb der ISO 27001 anhand von zwei Controls behandelt. Control A5.5 „Kontakt mit Behörden“ legt fest, dass es ein festes Verfahren geben sollte, welches definiert wer, wann und wie ein Vorfall an die zuständigen Behörden meldet. Control A.5.6 „Kontakt zu speziellen Interessensgruppen“ befriedigt im vorliegenden Fall die Verpflichtung, einen schwerwiegenden IKT-Vorfall dem Kunden zu melden. Zwar stehen in der Control selber Interessensgruppen im Fokus, welche sich mit der Thematik rund um Informationssicherheit auskennen („sicherheitsorientierte Expertenforen und Fachverbänden“), jedoch kann man durch die offene Formulierung der „speziellen Interessensgruppen“ ebenfalls auf Kunden schließen.
Die Meldung von Sicherheitsvorfällen, im Rahmen von dem IT-Grundschutz-Kompendium, wurde

bereits bei DORA.2.13 erläutert, jedoch spricht DORA.2.15 explizit von der Meldung an zuständige Aufsichtsbehörden. Dies wird alleinig durch DER.2.1.A4 „Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen“ behandelt. Hierbei wird die Meldung an alle relevanten internen und externen Stellen gefordert und explizit auch Meldungen an Behörden angesprochen.
Die Meldung schwerwiegender IKT-Vorfälle an entsprechend zuständige Behörden wird, durch den C5-Katalog, in SIM-03 „Dokumentation und Berichterstattung über Sicherheitsvorfällen“ und SIM-05 „Auswertung und Lernprozess“ thematisiert. Anders als ursprünglich vermutet wurde, findet OIS-05 „Kontakt zu relevanten Behörden und Interessensverbänden“ keine Anwendungen, da dieses Kriterium lediglich einen einseitigen Informationsfluss von Behörde/Interessensverband zum Cloud-Dienstleister zu Informationsgewinnung anspricht. SIM-03 hingegen spricht davon, einen Bericht, samt Lösung, zur Bestätigung an den Kunden zu übermitteln. Somit ist der geforderten Kundeninformation abgedeckt. Der Kontakt zu Behörden wird kurz in SIM-05 thematisiert. Hierbei werden Mechanismen zur Meldung an unterstützende Stellen, wie z.B. BSI, gefordert.

Zu DORA.2.14.1

Das Testen der operationellen Resilienz wird innerhalb der ISO 27001 nicht explizit durch eine Control behandelt, jedoch ergibt sich der Test der operationalen Resilienz durch die Anwendung von verschiedenen Controls. Zunächst fordert Control A.29 „Sicherheitsprüfung bei Entwicklung und Abnahme“, dass ein Prüfverfahren in den Entwicklungslebenszyklus integriert werden muss. Weiterhin fordert Control A8.29 „Trennung von Entwicklungs-, Test- und Produktionsumgebungen“, dass die im Titel genannten Umgebungen voneinander getrennt und gesichert werden müssen. Hierdurch wird die Existenz einer Testumgebung bereits impliziert. Schwachstellentests für IKT werden durch das IT-Grundschutz-Kompendium unter anderem durch die Anforderungen OPS.1.1.1.A22 „Automatisierte Tests auf Schwachstellen“ und OPS.1.1.1.A23 „Durchführung von Penetrationstests“ thematisiert. OPS.1.1.1.A22 stellt fordert hierbei, dass alle IT-Komponenten regelmäßig automatisiert überprüft werden sollten und die resultierenden Erkenntnisse weiterverwendet werden. Parallel fordert OPS.1.1.1.A23, dass ein Konzept zur manuellen Überprüfung von IT-Komponenten besteht, welches abhängig von der jeweiligen IT-Komponente eine individuelle Testtiefe berücksichtigt.
Aufseiten des C5-Katalogs werden Tests der operationalen Resilienz in OPS-19 „Umgang mit Schwachstellen, Störungen und Fehlern - Penetrationstests“ angesprochen. Hierbei wird eine mind. jährlich erfolgende Reihe von Penetrationstests gefordert.

Zu DORA.2.14.2

Die ISO 27001 verfügt über keine Controls, welche ein TLPT fordern. Aufseiten des IT-Grundschutz-Kompendiums kann die Anforderung OPS.1.1.1.A23 „Durchführung von Penetrationstests“ zu diesem Zweck herangezogen werden. Zwar spricht dieser nicht explizit von TLPT, jedoch resultiert aus dieser Anforderung ein Konzept für Penetrationstests, welches individuelle Testtiefen und -methoden zulässt.
Das TLPT wird durch den C5-Katalog nicht explizit angesprochen, jedoch kann OPS-19 „Umgang mit Schwachstellen, Störungen und Fehlern - Penetrationstests“ Anwendung finden, da hier die

geforderten Tests auf Grundlage einer definierten Testmethodik durchzuführen sind. Diese Definition wird nicht weiter ausgeführt, wodurch sich auch ein TLPT durchführen lässt.

Zu DORA.2.15

Das Management von IKT-Drittdienstleisterrisiken wird durch die ISO 27001 primär in den Controls A5.19 - A5.23 behandelt. Beginnend mit Control A5.19 „Informationssicherheit in Lieferantenbeziehungen“ werden Prozesse und Verfahren durch die Organisation entwickelt, welche dazu dienen Informationssicherheitsrisiken zu beherrschen, welche aus der Nutzung von Dienstleistungen oder Produkten resultieren. Konkret wird gefordert, dass z.B. festgelegt wird auf welche organisationsinterne IKT-Assets der Lieferant Zugriff hat. Damit das allgemeine Informationsicherheitsniveau auch aufseiten des Lieferanten gewahrt ist, sollten, durch die Umsetzung von Control A5.20 „Behandlung von Informationssicherheit in Liefervereinbarungen“, Lieferantenvereinbarungen getroffen werden. Die Control fordert hierbei unter anderem, dass ein einheitliches Klassifizierungsschema zwischen Organisation und Lieferant gehalten wird, wie auf Informationen zugegriffen wird oder auch, dass klare Regeln zur Nutzung von Informationen in der Lieferantenvereinbarung verankert werden. Die Control A5.21 „Umgang mit der Informationssicherheit in der IKT-Lieferkette“ geht weiter auf den Aspekt der IKT-Sicherheit ein und vertieft den Aspekt der Informationssicherheit in der gesamten IKT-Lieferkette. Die Control fordert unter anderem, dass die Informationssicherheitsanforderungen in der gesamten Lieferkette kommuniziert werden und sorgt für die Erarbeitung von Anforderungen für den Erwerb von IKT-Produkten. Ist eine Lieferantenvereinbarung getroffen, muss dieser durch die Organisation überwacht werden. Dies geschieht durch die Anwendung von Control A5.22 „Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen“. Neben weiteren Aspekten wird hierbei auf die allgemeine Vertragserfüllung hin überwacht bzw. überprüft oder es werden auch Informationssicherheitsaspekte in den Lieferantenbeziehungen des Lieferanten selber beleuchtet. Eine Studie der WIK-Consult GmbH aus dem Jahr 2022 hat gezeigt, dass bereits 90% der KMU Cloud-Dienste zur Datenspeicherung nutzen (vgl.[BAI24], S.7). Jedoch bietet die ISO 27001 auch für diesen Aspekt eine Control - A5.23 „Informationssicherheit für die Nutzung von Cloud-Diensten“ - an. Diese hilft dabei, dafür zu sorgen, feste Verfahren und Richtlinien für den Erwerb, die Nutzung, die Verwaltung und den Ausstieg aus Cloud-Diensten zu erarbeiten. Parallel zu der ISO27001 behandelt das IT-Grundschutz-Kompendium IKT-Drittdienstleistermanagement in dem Baustein OPS.2.3 „Nutzung von Outsourcing“. Hierbei werden anhand von 25 Anforderungen, schutzbedarfspezifische Aspekte der Informationssicherheit in Lieferantenbeziehungen betrachtet. Da alle vorliegenden Anforderungen zu der Erfüllung von DORA.2.17 beitragen, wird auf die Nennung der spezifischen Anforderungen verzichtet und der Baustein aufgelistet.

Die Steuerung, Überwachung, Dokumentation von Lieferantenbeziehungen wird durch den C5-Katalog innerhalb der SSO-Kriterienreihe angesprochen. Einleitend werden im Rahmen von SSO-01 „Richtlinien und Anweisungen zur Steuerung und Überwachung Dritter“ eine Reihe von Richtlinien und Anweisungen erarbeitet, welche unter anderem Vorgaben zur Risikobeurteilung, Vorgaben für die Klassifizierung von Dritten und Anforderungen an die Informationssicherheit berücksichtigen. Auf Grundlage dieser Richtlinien wird weiterhin durch SSO-02 „Risikobeurteilung der Dienstleister

und Lieferanten“ eine Risikobeurteilung der Lieferanten durchgeführt, um den Schutzbedarf der Informationen von Dritten zu identifizieren, Auswirkungen einer Schutzbedarfsverletzung auf den Cloud-Dienstleister zu identifizieren und Abhängigkeiten des Cloud-Dienstleister zum Lieferanten zu identifizieren. Alle Dienstleister und Lieferanten werden dabei in einem Verzeichnis erfasst, was diverse Identifikationsmerkmale zu dem Dienstleister und der erbrachten Leistung festhält (SSO-03 „Verzeichnis der Dienstleister und Lieferanten“). Die Überwachung der Dienstleister, im Bezug auf die Informationssicherheit, wird dabei durch Kriterium SSO-04 „Überwachung der Einhaltung der Anforderungen“ sichergestellt. Erkannte Verstöße gegen die Anforderungen werden automatisiert an die entsprechenden Systemkomponenten bzw. qualifizierte Personal, zur Beurteilung und Behebung, weitergeleitet. Sollte eine weitere Zusammenarbeit mit dem Dienstleister nicht mehr tragbar sein, kommt SSO-05 „Ausstiegsstrategien für den Bezug von Leistungen“ zum Einsatz. Hier werden diverse Ausstiegsstrategien auf Basis der BIA und BCM definiert.

4.3 KRITIS-DachG Konformität

Zu KRITIS-DachG.1

Die ISO 27001 verfügt über keinen keine Control, welche sich explizit mit der Registrierung bei den zuständigen Behörden beschäftigt. Im weiteren Sinne lässt sich jedoch die Control A.5.5 „Kontakt mit Behörden“ anwenden, da diese nicht nur die Kommunikation bei Informationssicherheitsvorfällen beschreibt, sondern den Informationsfluss im Ganzen (vgl. [DEU24b], 5.5). Aus gegebener Begründung wird diese Control mit der Kategorie T versehen.

Auch das IT-Grundschutz-Kompendium führt zu diesem Zweck keinen spezifischen Baustein an, da dieser vorwiegend die IKT-Systeme betrachtet und das dahingehende Management. Der Baustein ORP.5 „Compliance Management“ beschäftigt sich jedoch unter anderem auch mit rechtlichen Anforderungen. Die Anforderung ORP.5.A1 „Identifikation der Rahmenbedingungen“ schreibt hierzu vor, dass alle rechtlichen Anforderungen erfasst werden müssen. In Verbindung mit der darauffolgenden Anforderung ORP.5.A2 „Beachtung der Rahmenbedingungen“, welche Führungskräfte zur unternehmensweiten Einhaltung der erfassten Rahmenbedingungen verpflichtet, ist jedoch davon auszugehen, dass bei richtiger Umsetzung eine Konformität erlangt werden kann. Beide Anforderung erhalten die Kategorie T.

Aufseiten des C5-Kriterienkatalogs wird es noch schwerer eine passende Maßnahme auszumachen. Dieser verfügt mit OIS-05 „Kontakt zu relevanten Behörden und Interessensverbänden“, jedoch konkretisiert dieses Kriterium den Kontakt insofern, als dieser zum Zwecke der Informationsgewinnung über Schwachstellen und Gefährdungen dient. In Folge konnte kein konkretes Kriterium für diese Anforderung ausgemacht werden.

Zu KRITIS-DachG.2

Die ISO 27001 verfügt über keine Control, welche sich mit einer regelmäßigen Risikoanalyse beschäftigt. Man kann argumentieren, dass eine regelmäßige Risikoanalyse ein Teil der Informations-

sicherheitsleitlinie und -politik sein sollte und somit über die Control A.5.1 geführt werden kann, jedoch zeigen dies weder die ISO 27001, noch die Ausführungen der ISO 27002 auf. Somit wird keine Maßnahme zur Bewältigung ausgewählt. Die Risikoanalyse wird im IT-Grundschutz-Kompendium nicht als einzelner Baustein aufgeführt, sondern wird von dem Anwender vorausgesetzt. Die Risikoanalyse erfolgt im IT-Grundschutz in der Publikation BSI 200-3 „Risikomanagement“ ([BUN17c]) thematisiert. Somit wird keine Bausteinanforderung diesbezüglich ausgewählt. Im Gegensatz zu der ISO 27001 und dem IT-Grundschutz-Kompendium, führt der C5-Kriterienkatalog mit dem Kriterium OIS-06 „Richtlinie für den Umgang mit Risiken“ ein Kriterium, welches sich konkret mit der Identifikation, der Analyse, der Bewertung, der Behandlung und der Dokumentation von Risiken beschäftigt. Gepaart mit dem Kriterium SP-01 „Dokumentation, Kommunikation und Bereitstellung von Richtlinien und Anweisungen“, welches Rahmenbedingungen für abgeleitete Richtlinien festlegt, kann bei Umsetzung eine Konformität erreicht werden. Es wird für beide Kriterien die Kategorie T vergeben.

Zu KRITIS-DachG.3.1.1

Da es sich bei dem KRITIS-DachG um eine Verordnung handelt, welche vorwiegend die physische Resilienz stärken will, muss dieser physischer Aspekt bei der Auswahl der Maßnahmen berücksichtigt werden.

Die ISO 27001 beschreibt mit der Control A.7.5 „Schutz vor physischen und umweltbedingten Bedrohungen“ Maßnahmen, welche umweltbedingte oder physische Bedrohungen verhindern oder verringern sollen. Da in der gesetzlichen Anforderung konkret Maßnahmen im Bezug auf den Klimawandel gefordert werden, kann diese Control zu einer Konformität beitragen. Somit wird die Kategorie T vergeben.
Das IT-Grundschutz-Kompendium führt keinen Baustein auf, welcher konkret den Klimawandel bzw. umweltbedingte Bedrohungen adressiert, da es hauptsächlich die IKT-Systeme betrachtet.

Zu KRITIS-DachG.3.1.2

Die ISO 27001 führt eine Reihe von Controls auf, welche auf den physischen Schutz der jeweils betrachteten Assets abzielt. Angefangen bei A.7.1 „Physischer Sicherheitsperimeter“ wird der Perimeter betrachtet und im Anschluss mit der folgenden Controls immer weiter ins Detail gegangen, bis mit A.7.8 die „Platzierung und Schutz von Geräten und Betriebsmitteln“ thematisiert wird. Bei Umsetzung dieser Maßnahmen kann eine Konformität mit der Anforderung erreicht werden, weshalb für jede einzelne Control die Kategorie T vergeben wird.
Das IT-Grundschutz-Kompendium weist gegenüber der ISO 27001 eine deutlich ausgedehntere Betrachtung des physischen Schutzes auf. Baustein INF.1 „Allgemeines Gebäude“ beschreibt den physischen Schutz der Liegenschaft anhand von 31 Anforderungen (lückenhaft von INF.1.A1 bis INF.1.A35) sehr ausführlich. Für jede einzelne Anforderung innerhalb dieses Bausteins wird die Kategorie T vergeben, während der Baustein als solcher die Kategorie V erhält.
Für den Schutz der Liegenschaft wurden im C5-Kriterienkatalog drei konkrete Kriterien ausgemacht. Beginnend mit dem Kriterium PS-03 „Perimeterschutz“ wird der physische äußere Schutz adressiert. Weiterhin wird im darauffolgendem Kriterium PS-04 „Zutrittskontrollen“ eine weitere Ebene

an physischen Schutz eingepflegt. Diese beiden Kriterien bieten ausreichende Ausführungen, um den geforderten Objektschutz bzw. Schutz der Liegenschaft zu gewährleisten. Es wird jeweils die Kategorie T vergeben.

Zu KRITIS-DachG.3.1.3

Die Reaktion auf Informationssicherheitsvorfälle wird, durch die ISO 27001, in der Control 5.26 „Reaktion auf Informationssicherheitsvorfälle“ adressiert. Hierzu werden feste Verfahren zur Reaktion auf Vorfälle bestimmt und festgehalten. Auch wenn diese Control als solches vermutlich bereits ausreichend ist, um der gesetzlichen Anforderung Genüge zu tun, sollte beachtet werden, dass bei einem Informationssicherheitsvorfall die Informationssicherheit bei einem Vorfall auf einem angemessenen Niveau bleibt. Hierzu bietet Control A.5.29 „Informationssicherheit bei Störungen“, in Verbindung mit A.5.30 „IKT-Bereitschaft für Business-Continuity“ einen Ansatz, um dies zu gewährleisten. Da A.5.26 bereits als solches die Reaktion als solche vollumfänglich adressiert, wird Kategorie V vergeben. Für A5.29 und A5.30 werden als zusätzliche Controls die Kategorie T vergeben.
Das IT-Grundschutz-Kompendium bietet mindestens zwei Bausteine, welche die Reaktion auf Informationssicherheitsvorfälle beleuchtet. Beginnend werden mit Baustein DER.2.1 „Behandlung von Sicherheitsvorfällen“, anhand von 22 Anforderungen, ein Rahmen für die Reaktion gelegt. Weiterhin wird im Baustein DER.2.3 „Bereinigung weitreichender Sicherheitsvorfälle“ die Reaktion auf Vorfälle adressiert, welche auf einem sehr fortgeschrittenen technischen Stand sind. Diese beiden Bausteine werden mit dem Baustein DER.4 „Notfallmanagement“ abgerundet, welcher bei Ausfall von Systemen oder Personen greift. Da grundsätzliche Informationssicherheitsvorfälle durch den Baustein DER.2.1 bereits ausreichend adressiert werden, wird für diesen die Kategorie V vergeben. DER.2.1 und DER.4 erhalten aufgrund ihres komplementierenden Charakters die Kategorie T.
Der C5-Kriterienkatalog adressiert den Umgang mit Sicherheitsvorfällen in mehreren Kriterien, welche einander komplettieren. Zunächst werden in Kriterium SIM-01 „Richtlinie für den Umgang mit Sicherheitsvorfällen“ feste Verfahren festgelegt. Kriterium SIM-02 „Bearbeitung von Sicherheitsvorfällen“ legt fest, wie eine Klassifizierung, Priorisierung und Ursachenanalyse eines gegebenen Vorfalls durchzuführen ist. Für diesen Vorgang wird, auf Grundlage des Kriteriums SIM-03 „Dokumentation und Berichterstattung über Sicherheitsvorfälle“, eine adäquate Dokumentation durchgeführt. Da sich diese Kriterien gegenseitig ergänzen und in einzelner Form die Reaktion auf einen Vorfall nicht ausreichend beleuchten, wird jeweils Kategorie T vergeben.

Zu KRITISDachG.3.1.4

Diese Anforderung beschäftigt sich mit der Aufrechterhaltung und Wiederherstellung des Betriebs, nach einem Vorfall. Es handelt sich also um klassisches BCM.

Die ISO 27001 behandelt das BCM in den Controls A5.29 „Informationssicherheit bei Störungen“ und A5.30 „IKT-Bereitschaft für Business-Continuity“. A5.29 gibt hierbei vor, dass ein „angemessenes Niveau“ gewahrt werden soll. Weitere Definitionen bleiben in der Norm aus. Folglich definiert sich das angemessene Niveau aus den organisationsinternen Sicherheitszielen. Ist ein angemessenes

Niveau für die Organisation definiert, sollte im nächsten Schritt überlegt werden, welche Assets im Notfall priorisiert werden sollten. Hier setzt die Control A5.30 an. Diese beschreibt einen Analyseprozess, welcher im Anschluss zu konkreten Ableitungen für IKT-Kontinuitätspläne, um eine stetige Verfügbarkeit der unternehmensinternen Informationen zu gewährleisten. Da Control A5.30 eine weiterführende Maßnahme von A5.29 darstellt, erhält A5.30 die Kategorie T und A5.29 die Kategorie V.
Aufseiten des IT-Grundschutz-Kompendiums wird das Thema des BCM durch den Baustein DER.4 „Notfallmanagement“ thematisiert. Grundlegend ist hierbei die Standard-Anforderung DER.4.A1 „Erstellung eines Notfallhandbuchs“, welche unter anderem die gesetzlichen geforderten Maßnahmen definiert. Neben dieser elementaren Anforderung zum BCM, werden im weiteren Verlauf des Bausteins noch zusätzliche Aspekte beleuchtet, welche einem höheren Schutzbedarf entsprechen. DER.4.A1 erfüllt jedoch bereits die gesetzliche Anforderung KRITIS-DachG.3.1.4, wodurch die Kategorie V vergeben wird.
Der C5-Katalog widmet dem Thema des BCM eine Familie an Kriterien, welche im Gesamten zu einem effektiven BCM führen. Angefangen mit BCM-01 **Verantwortung durch die Unternehmensleitung!** (**Verantwortung durch die Unternehmensleitung!**) wird ein grundlegendes Verständnis der Rolle der Unternehmensleitung gelegt. Im Anschluss wird im Rahmen von BCM-02 „Richtlinien und Verfahren zur Business Impact Analyse“ eine Methodik (Richtlinien, Anweisungen) entwickelt, um Auswirkungen von Störungen zu ermitteln. Aufgrund der gewonnenen Erkenntnisse kann anhand von BCM-03 „Planung der Betriebskontinuität“ ein Rahmenwerk entwickelt werden, welches als Resultat konkrete Pläne zur Betriebskontinuität hervorbringt. Damit diese Pläne stets an die aktuelle Bedrohungslage und auf dem aktuellen Stand der Technik ist, werden diese mittels BCM-04 „Verifizierung, Aktualisierung und Test der Betriebskontinuität“ überprüft. Da jedes einzelne Kriterium selbstständig nicht im vollen Umfang der gesetzlichen Anforderung genügt, wird jeweils die Kategorie T vergeben.

Zu KRITIS-DachG.3.1.5

Diese Anforderung beschäftigt sich mit dem Sicherheitsmanagement im Hinblick auf das Personal. Beispielhaft werden hierfür sowohl Zugangsrechteverwaltung, also technische Systemanforderungen, als auch persönliche Qualifikationen und Sicherheitsüberprüfungen angeführt. Dementsprechend kann hierzu ein breites Spektrum an Maßnahmen getroffen werden.

Zu den technischen Aspekten dieser gesetzlichen Anforderung liefert die ISO 27001 eine Control, welche exakt die beispielhaft angeführte Zugangsrechteverwaltung abdeckt. Die Control A5.18 „Zugangsrechte“ beschäftigt sich im Kern damit, wie der Zugang zu Informationen beschränkt werden kann. Hierbei wird die gesamte Zeitspanne von Erteilung, über Überprüfung bis hin zur Entziehung der Zugangsrechte beleuchtet. Diese wird durch die Control A8.3 „Informationszugangsbeschränkung“, um weitere technische Aspekte ergänzt. Auch zur beispielhaften Sicherheitsüberprüfung liefert die ISO 27001 eine passgenaue Control. Die Control A6.1 „Sicherheitsüberprüfung“ gibt vor, dass bei Einstellung von neuem Personal eine Überprüfung erfolgen sollte, damit sichergestellt ist, dass

diese ihre künftigen Aufgaben adäquat erfüllen kann. Da alle angeführten Controls die gesetzliche Anforderung nicht im Einzelnen vollständig erfüllen, wird Kategorie T vergeben.
Das IT-Grundschutz-Kompendium widmet sich solchen personellen Aspekten primär in dem Baustein ORP „Organisation und Personal“. Interessant für diese rechtliche Anforderung ist hierbai der Baustein ORP.4 „Identitäts- und Berechtigungsmanagement“. Dieser widmet sich den angeführten technischen Beispielen, wie die Zugangsrechteverwaltung und Festlegung von Personalkategorien. Dabei werden ebenfalls Anforderungen angeführt, welche die angeführten gesetzlichen Beispiele Genüge tun. So kann wird in ORP.4.A1 eine Regelung zur Erstellung von Benutzenden und Benutzendengruppen (vgl. [BUN24c], Art. 10, (2) 1. a) aa)) erstellt. Diese beschreibt jedoch lediglich ein generelles Vorgehen zu der Erstellung und differenziert somit nicht zwischen den Funktionen. Diese Trennung wird in ORP.4.A4 „Aufgabenverteilung und Funktionstrennung“ vorgenommen. Die beispielhaft angeführte Zugangsberechtigungseinschränkung zur Liegenschaft und Informationen (vgl.[BUN24c], Art.10, (2) 1. a) bb)) wird durch die Anforderungen ORP.4.A5 „Vergabe von Zutrittsberechtigungen“, ORP.4.A6 „Vergabe von Zugangsberechtigungen“ und ORP.4.A7 „Vergabe von Zugriffsrechten“ ausreichend abgedeckt. Weiterhin spricht die gesetzliche Anforderung von „Zuverlässigkeitsprüfungen“ (vgl.[BUN24c], Art.10, (2) 1. b)). Diese werden im Baustein ORP.2 „Personal“ beschrieben. Dabei stellen konkret ORP.2.A7 „Überprüfung der Vertrauenswürdigkeit von Mitarbeitenden“ und ORP.2.A13 „Sicherheitsüberprüfung“ die jeweilige Überprüfung des Mitarbeitenden, gemäß dem Schutzbedarf, sicher.
Der C5-Katalog bietet grundsätzlich zwei Kriterien, welche für die Erfüllung der Anforderung herangezogen werden können - namentlich IDM-01 „Richtlinie für Zugangs- und Zugriffsberechtigungen“ und HR-01 „Überprüfung der Qualifikation und Vertrauenswürdigkeit“. IDM-01 erfüllt hierbei die technischen Anforderungen und behandelt sowohl die physische Zugangsberechtigung, als auch die digitale Zugriffsberechtigung. HR-01 beschreibt hingegen Kriterien zur Überprüfung der Qualifikationsangaben und schreibt unter anderem eine „Bewertung der Erpressbarkeit“ vor (vgl. [BUN20a], HR-01). Durch die Berücksichtigung beider Kriterien kann der gesetzlichen Anforderung bereits Genüge getan werden.

Zu KRITIS-DachG.3.1.6
Da das Personal eines Unternehmens zu meist der treibende Faktor bei dem Wirtschaften ist, ist es fundamental wichtig das Personal angemessen zu schulen und zu sensibilisieren. Auch das KRITIS-DachG erkennt dies an und fordert dies vom Anwender.

Die ISO 27001 geht auf die Schulung und Sensibilisierung von Personal in der beinahe gleichnamigen Control A6.3 „Informationssicherheitsbewusstsein, -ausbildung und -schulung“ ein. Diese schreibt vor, dass es eine geeignete Richtlinie vorhanden ist, welche sicherstellt, dass Personal sich ihrer Verantwortung bewusst ist und dementsprechend geschult wird.
Das IT-Grundschutz-Kompendium widmet diesem Thema nicht nur eine Maßnahme, sondern einen ganzen Baustein - ORP.3 „Sensibilisierung und Schulung zur Informationssicherheit“. Hier werden mehrere Aspekte bzw Ansätze zum Informationssicherheitsbewusstsein beleuchtet. Beginnend mit

ORP.3.A3 „Einweisung des Personals in den sicheren Umgang mit IT“ wird dem Mitarbeiter ein grundsätzlich sicherer Umgang mit Informationstechnologie beigebracht. Darüber hinaus fordert ORP.3.A4 „Konzeption und Planung eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit“, die Konzeption eines zielgruppenorientierten Programmes, um das Personal auf einem angemessenen Wissensstand, bezüglich der Informationssicherheit, zu halten. Die praktische Umsetzung von Schulungen wird in ORP.3.A6 „Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit“ gefordert. Über die aufgezeigten Anforderungen hinaus bietet das Kompendium noch weitere Anforderungen, welche sich jedoch an die Institutionsleitung, Informationssicherheitsbeauftragte oder sich an einen erhöhten Schutzbedarf orientieren und somit in erster Linie für die grundsätzliche Erfüllung der gesetzlichen Anforderung uninteressant sind.
Der C5-Katalog schreibt mit dem Kriterium HR-03 „Programm zur Sicherheitsausbildung und Sensibilisierung“ vor, dass ein solches, an der Informationssicherheitsleitlinie orientiertes, Programm a) existieren muss und b) jeder interner und externe Mitarbeiter dies regelmäßig durchlaufen muss. Da die rechtliche Formulierung von „angemessen“ spricht, wird durch die Erfüllung dieses Kriteriums der Anforderung bereits Genüge getan.

Zu KRITIS-DachG.3.2

Die Dokumentation von den angewandten Maßnahmen ist ein essenzieller Bestandteil der Unternehmensresilienz. Die angefertigte Dokumentation dient bei Prüfungen zur Nachvollziehbarkeit der getroffenen Maßnahmen. Diesbezüglich wird von dem Kritis-DachG dementsprechend ein Dokument gefordert - der Resilienzplan -, welcher die getroffenen Maßnahmen übersichtlich an einem Punkt dokumentiert.

Die ISO 27001 führt keine spezielle Control an, welche sich damit beschäftigt eine Dokumentation von allen getroffenen Maßnahmen anzufertigen. Stattdessen wird oft in der Konzeption der Maßnahmen, welche ein Unternehmen treffen will, bereits Augenmerk darauf gelegt, dass dies angemessen dokumentiert wird. Die aus der Control A5.1 „Informationssicherheitspolitik und -richtlinien“ entspringenden Richtlinien, kommt einem Resilienzplan am nächsten. Hier sollen themenspezifische Richtlinien zu den Themen der Zugangssteuerung, physische und umgebungsbezogenen Sicherheit, Verwaltung der Werte, Informationsübertragung, sichere Konfiguration und Handhabung von Benutzerendpunktgeräten, Netzwerksicherheit, Handhabung von Informationssicherheitsvorfällen, Datensicherung, Kryptographie und Schlüsselverwaltung, Informationsklassifizierung und deren Handhabung, Handhabung von technischen Schwachstellen und der sicheren Entwicklung geschaffen werden. Diese sollen ebenfalls Maßnahmen anordnen, welche im Rahmen des angesprochenen Themas getroffen werden (vgl. [DEU24b], 5.1). Diese themenspezifische Richtlinien können entsprechend ein guter Ausgangspunkt sein, um die Informationen daraus in die gesetzlich geforderte Form des Resilienzplans zu überführen.
Das IT-Grundschutz-Kompendium verfügt über mehrere, in den jeweiligen Bausteinen verankerten, Konzeptionsphasen. Hierbei wird innerhalb der Basis-Anforderungen bereits eine Dokumentation gefordert. Grundlegend für dieses Vorgehen ist die Anforderung ISMS.1.A7 „Festlegung von Sicher-

heitsmaßnahmen“, welche die systematische Dokumentation in Sicherheitskonzepten fordert. Die resultierenden Informationen können ein Startpunkt für die Überführung in das geforderte gesetzliche Format darstellen.
Der C5-Katalog ähnelt in diesem Fall dem IT-Grundschutz-Kompendium. Es wird über das Kriterium SP-01 „Dokumentation, Kommunikation und Bereitstellung von Richtlinien und Anweisungen“ gefordert, dass von der Informationssicherheitsrichtlinie abgeleitete Richtlinien bereits die *„Maßnahmen zur Umsetzung der Sicherheitsstrategie“* dokumentiert werden.

Zu KRITIS-DachG.4
Die ISO 27001 enthält keine konkrete Control, welche die Nachweiserbringung zur Erfüllung von gesetzlichen Anforderungen fordert. Es kann sich jedoch im weiteren Sinne auf zwei Controls bezogen werden. Control A5.31 „Juristische, gesetzliche, regulatorische und vertragliche Anforderungen“ fordert, dass die Erfassung und Einhaltung von allen rechtlichen Anforderungen. Da es sich bei der Nachweiserbringung um eine solche rechtliche Anforderung handelt, muss die Erbringung, durch die Anwendung von dieser Control, erbracht werden. Gepaart mit dem, aus der Control A5.5 „Kontakt mit Behörden“, Informationsfluss, kann die Nachweiserbringung gewährleistet werden.
Das IT-Grundschutz-Kompendium widmet sich dieser Anforderung implizit durch die Anwendung des Bausteines ORP.5 „Compliance Management“. Hier fordert die Basis-Anforderungen ORP.5.A1 „Identifikation der Rahmenbedingungen“, dass gesetzliche Rahmenbedingungen identifiziert und dokumentiert werden. In Verbindung mit ORP.5.A2 „Beachtung der Rahmenbedingungen“, welche Führungskräfte dazu verpflichtet für die Einhaltung der identifizierten Rahmenbedingungen zu sorgen, kann die Nachweiserbringung gewährleistet werden.
Auch der C5-Katalog verfügt über ein Kriterium, welches der Anforderung gerecht werden kann. Das Kriterium COM-01 „Identifizierung anwendbarer gesetzlicher, regulatorischer, selbstauferlegter oder vertraglicher Anforderungen“ fordert - ähnlich wie beim IT-Grundschutz-Kompendium -, dass die gesetzlichen Anforderungen identifiziert und zusammen mit Verfahren zur Einhaltung dokumentiert werden. **Zu KRITIS-DachG.5**
Mit der Verabschiedung des KRITIS-DachG werden erneut Meldefristen für Betreiber kritischer Anlagen festgelegt.

Die ISO 27001 verfügt zu dem Zweck der Meldung von Informationssicherheitsvorfällen an zuständige Behörden über die Control A5.5 „Kontakt zu Behörden“. Diese fordert, dass dokumentiert werden muss, Wer, Wann und Wie dafür zuständig ist, die Behörden über einen Informationssicherheitsvorfall zu informieren. Dies wird darüber hinaus in Control A5.24 „Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen“ spezifiziert. Hier wird die Planung von festen Verfahren zur unter anderem Koordinierung mit externen Stellen gefordert.
Das IT-Grundschutz-Kompendium enthält mit dem Baustein DER.2.1 „Behandlung von Sicherheitsvorfällen“ über zwei grundlegende Anforderungen zu dem Zweck der Meldung an Dritte bzw. offizielle Stellen. Zunächst wird in der Basis-Anforderung „Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen“ gefordert, dass alle interne und externen Stellen bei einem Sicherheitsvorfall

informiert werden müssen. Es wird ebenfalls explizit gefordert, dass Meldepflichten zu Aufsichtsbehörden eingehalten werden müssen. Diese Anforderung ist selbstständig schon dazu in der Lage, KRITIS-DachG.5 Genüge zu tun, jedoch wird auf tieferer Ebene mit der Standard-Anforderung DER.2.1.A9 „Festlegung von Meldewegen“ gefordert, dass festzulegen ist, wer solche Informationen an Dritte weitergibt.
Für den C5-Katalog konnte in diesem Fall kein spezifisches Kriterium zur Erfüllung ausgemacht werden. Der Katalog verfügt über diverse Kriterien, welche zur Meldung von Sicherheitsvorfällen verpflichten, jedoch diese Verpflichtung nur für intern für Mitarbeiter oder für Kunden, welche Sicherheitsvorfälle an eine zentrale Stelle melden sollen (vgl. [BUN20a], SIM-04). Auch das Kriterium OIS-05 „Kontakt zu relevanten Behörden und Interessensverbänden“ findet hier keine Anwendung, da dieses einen Kontakt lediglich zur Gewinnung von Informationen über aktuelle Schwachstellen und Gefährdungen beschreibt (vgl. [BUN20a], OIS-05). Das einzige Kriterium, welches sich hiermit befasst, ist COM-01 „Identifizierung anwendbarer gesetzlicher, regulatorischer, selbstauferlegter oder vertraglicher Anforderungen“, welches die Identifizierung und Einhaltung von gesetzlichen Anforderungen fordert.

Zu KRITIS-DachG.6.1

Da es für eine hinreichende Resilienz zwingend notwendig ist, dass die Organisationsleitung den getroffenen Maßnahmen zustimmt und aktiv bei der Umsetzung unterstützt, fordert das Gesetz durch diese Anforderung ein genau solches Verhalten.
Die ISO 27001 widmet sich diesem Aspekt in den Controls A5.1 „Informationssicherheitspolitik und -richtlinien“ und A5.4 „Verantwortlichkeiten der Leitung“. Ersteres legt hierbei dar, dass die Informationssicherheitspolitik von der obersten Leitung genehmigt ist und diese Ansätze zur Erfüllung darlegt. Letzteres zeigt auf, dass die Leitung dafür zuständig ist, die Umsetzung der Maßnahmen durch das Personal sicherzustellen.
Im Rahmen des IT-Grundschutz-Kompendium legt die Anforderung ORP.5.A2 „Beachtung der Rahmenbedingungen“ fest, dass Führungskräfte für die Umsetzung der rechtlichen oder sonstigen Anforderungen zuständig sind. Da die ultimative Führungskraft die Geschäftsleitung ist, ist KRITIS-DachG.6.1 Genüge getan.
Der C5-Katalog schreibt mit der Anforderung COM-03 „Interne Audits des Informationssicherheitsmanagementsystems“ vor, dass mindestens einmal jährlich die Umsetzung von gesetzlichen Maßnahmen, durch qualifiziertes Personal, kontrolliert wird. Es ist davon auszugehen, dass die Geschäftsleitung dazu qualifiziert ist und insofern wird dem geforderten „Überwachen“ Genüge getan. Der Billigungsteil wird durch SP-01 „Dokumentation, Kommunikation und Bereitstellung von Richtlinien und Anweisungen“ implizit Genüge getan, indem diese Anforderung beschreibt, dass Richtlinien und Anweisungen durch die oberste Leitung genehmigt werden.

Zu KRITIS-DachG.6.2

Schulungen werden von der ISO 27001 durch die Control A.6.3 „Informationssicherheitsbewusstsein, -ausbildung und -schulung“ adressiert. Es sollen laut dieser Control regelmäßige Schulungen

stattfinden und trifft somit auf NIS2UmsuCG.6.2 zu. Eine Hürde bei der Anwendung dieser Control liegt jedoch im Sprachgebrauch der Control. Bei den Ausführungen in der ISO 27002 beschreibt die Control lediglich das Personal der Organisation. Zur passenden Anwendung ist es folglich notwendig zu definieren, ob die Geschäftsleitung ebenfalls Personal der Organisation ist oder einen anderen Status innehat. Aufgrund der vorherigen Begründung erhält diese Control jedoch die Kategorie V.
Im Gegensatz zu der ISO 27001 adressiert das IT-Grundschutz-Kompendium die Sensibilisierung und Schulung der Geschäftsleitung explizit. Dies ist in der Anforderung ORP.3.A1 „Sensibilisierung der Institutionsleitung für Informationssicherheit“ festgehalten, welche die Vorgesetzten zum Vorangehen bei Schulungsmaßnahmen verpflichtet. Entsprechend wird die Kategorie V zugewiesen.
Für den C5-Katalog gilt selbige Problematik, wie für die ISO 27001. Hier wird in Anforderung HR-03 „Programm zur Sicherheitsausbildung und Sensibilisierung“ zwar Schulungen für interne Mitarbeiter gefordert, jedoch ist selbstständig zu klären, ob die Geschäftsleitung ein Mitarbeiter ist. Es wird dennoch die Kategorie V zugewiesen.

4.4 NIS2UmsuCG Konformität

Zu NIS2UmsuCG.1.2
Durch die offene Formulierung der „Konzepte in Bezug auf die Risikoanaylse und auf die Sicherheit in der Informationstechnik“ ([BUN24b], Art.30 Abs.2 Satz 1) wird ein weiter Rahmen für die Erfüllung dieser Anforderung gegeben.

Die ISO 27001 behandelt die Risikoanalyse in den Kapiteln 6.1 „Maßnahmen zum Umgang mit Risiken und Chancen “, 8.2 „Informationssicherheitsrisikobeurteilung “ und 8.3 „Informationssicherheitsrisikobehandlung “ thematisiert werden, betrifft das geforderte Konzept zur Sicherheit in der Informationstechnik im Grunde genommen alle Kapitel von 4.1 bis 10.2. Diese Kapitel bieten im Gesamten Sicherheit für die Informationstechnik in der Organisation.
Eine konkrete Control zur Erfüllung stellt die Control A.5.1 „Informationssicherheitspolitik und -richtlinien “ dar, da diese sowohl die Risikoanalyse, als auch technische Maßnahmen zur Sicherheit in der Informationstechnik einschließt. Aus diesem Grund erhält diese Control die Kategorie V im Katalog.
Bezüglich des IT-Grundschutz-Kompendiums lässt sich sagen, dass aufgrund der offenen Formulierung der Risikomanagementmaßnahmen sich hier erneut kein passgenauer Baustein ermitteln. Da es sich hierbei jedoch primär um die Herstellung von Prozessen zur Informationssicherheit geht lässt sich Baustein ISMS.1 „Sicherheitsmanagement“ anwenden, da sich dieser mit der Herstellung von Informationssicherheit und dem damit einhergehenden kontinuierlichen Prozess der Aufrechterhaltung beschäftigt. Weiterhin sind Bausteine denkbar, welche sich mit technologischen Maßnahmen zur Sicherheit der Informationssysteme, denkbar. Hier können SYS und OPS Bausteine Anwendung finden.

Auch beim C5-Katalog kann, aufgrund der offenen Formulierung, keine genaue Zuordnung stattfinden. Thematisch behandeln Baustein OIS-02 „Leitlinie zur Informationssicherheit“, SP-01 „Dokumentation, Kommunikation und Bereitstellung von Richtlinien und Anweisungen“, sowie SP-02 „Überprüfung und Freigabe von Richtlinien und Anweisungen“ Richtlinien zur Informationssicherheit und können hier entsprechend Anwendung finden.

Zu NIS2UmsuCG.1.3

Auf diese Anforderung lässt sich jede Maßnahme anwenden, welche dazu beiträgt einen Sicherheitsvorfall zu „bewältigen“. Die Bewältigung schließt hierbei die Detektion und Prävention mit ein.

Auf Seiten der ISO 27001 Controls lässt sich zunächst A.5.24 „Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen“ anwenden, da diese bei Umsetzung einen Rahmen zur schnellen und organisierten Reaktion bereitstellt. Darauf folgt Control A.5.25 „Beurteilung und Entscheidung über Informationssicherheitsereignisse“, welche bei richtiger Umsetzung einen Prozess bereitstellt, um den Sicherheitsvorfall zu kategorisieren und zu priorisieren. Control A.5.26 „Reaktion auf Informationssicherheitsvorfälle“ stellt die eigentliche technische und Hands-on Reaktion des Informationssicherheitsteams dar. Sobald der Sicherheitsvorfall entsprechend behandelt wurde, kann mit der Nachbereitung des Sicherheitsvorfalls begonnen werden, was ebenfalls zum Bewältigungsprozess gehört. Hierzu geben die Controls A.5.27 „“ A.5.28 „Sammeln von Beweismaterial“ einen Prozess vor, wie mit den gesammelten Beweisen zu verfahren ist, damit evtl. ein gerichtlicher Prozess eingeleitet werden kann.
Da A5.24, A.5.25, A.5.27 und A.5.28 jeweils entweder der Vor- oder Nachbereitung des Sicherheitsvorfalls angehören, erhalten diese Controls die Kategorie T. A.5.26 erhält als technische Reaktion auf den Sicherheitsvorfall die Kategorie V.
Das IT-Grundschutz-Kompendium behandelt die Bewältigung von Sicherheitsvorfällen in den Bausteinen DER.2.1 „Behandlung von Sicherheitsvorfällen“ und DER.2.3 „Bereinigung weitreichender Sicherheitsvorfälle“thematisiert und kann somit passgenau angewendet werden.
Der C5 Katalog bietet zu diesem Thema die Bausteine SIM-01 bis SIM-05. Beginnend mit einer „Richtlinie für den Umgang mit Sicherheitsvorfällen“, über die „Bearbeitung von Sicherheitsvorfällen“, bis hin zur „Auswertung und Lernprozess“ wird dies thematisiert.

Zu NIS2UmsuCG.1.4

Diese Anforderung beschäftigt sich, wie im Anhang A, aufgezeigt mit der Aufrechterhaltung und Wiederherstellung des Betriebs, sowie dem Krisenmanagement. In anderen Worten können zur Konformität diejenigen Maßnahmen herangezogen werden, welche das BCM betreffen.

Die ISO 27001 gibt diesbezüglich eine Reihe von Controls an. Die Control A.5.29 „Informationssicherheit bei Störungen“ beschäftigt sich mit der Planung der Informationssicherheit während einer Störung, damit diese auf einem angemessenem Niveau erhalten bleibt. Weiterhin beschäftigt sich die Control A.5.30 „IKT-Bereitschaft für Business-Continuity“ mit der Verfügbarkeit von Infor-

mationen und Assets während einer Störung und ist somit ebenfalls geeignet, um zu der Konformität beizutragen.
Bezüglich des konkret genannten Backup-Management und Krisenmanagement liefert die ISO 27001 die Controls A.8.13 „Sicherung von Informationen“ und A.8.14 „Redundanz von informationsverarbeitenden Einrichtungen“. Während ersteres die Erstellung von Sicherheitskopien von Informationen zur Informationswiederherstellung adressiert, beschäftigt sich letzteres mit der Systemwiederherstellung und gibt beispielsweise vor die Systemarchitektur so zu planen, dass im Störungsfall ein redundantes System die ausgefallene Funktion übernehmen kann.
Aufgrund der vorangestellten Ausführung erhalten alle benannten Controls die Kategorie T im Katalog, da diese als einzelnes die Anforderung nicht vollumfänglich erfüllen.
Da es sich bei dieser Maßnahme um Business-Continuity handelt, kann Baustein DER.4 „Notfallmanagement“ aus dem Kompendium herangezogen werden.
Der C5-Katalog bietet, mit den Bausteinen BCM-01 bis BCM-04 , eine umfassende Beleuchtung der Gesichtspunkte zum Thema des Business-Continuity.

Zu NIS2UmsuCG.1.5
Diese Anforderung ist in der Umsetzung eine sehr hohe Anforderung, da hier die jeder Anbietet oder Dienstleister eines Unternehmens von jenem Unternehmen kontrolliert werden muss, um die Sicherheit der Lieferkette zu gewährleisten. Aufgrund der Verwendung von „unmittelbaren“, im Gesetzestext, wird zur weiteren Bearbeitung die Annahme getroffen, dass nur die Anbieter/Dienstleister in der ersten Ebene kontrolliert werden müssen, nicht jedoch deren Anbieter.

Zu dem Zweck der Lieferkettensicherheit bzw. dem Lieferkettenmanagement bietet die ISO 27001 fünf Controls an. Anfänglich führt die Control A.5.19 „Informationssicherheit in Lieferantenbeziehungen“ feste Prozesse und Verfahren zur Informationssicherheit ein und bewerkstelligt, dass es eine dokumentierte und kommunizierte Richtlinie für Lieferantenbeziehungen gibt. Weiterhin
Für diese Maßnahme konnte kein passender Baustein ausgemacht werden. Im weitesten Sinne kann hier der Baustein OPS.2.3 „Nutzung von Outsourcing“ angewandt werden, da hier ein Geschäftsprozess vom eigenen Unternehmen an ein anderes Unternehmen (Dienstleister, Lieferant von Leistungen) übergeben wird.
Das Risikomanagement, im Bezug auf die Lieferkette, wird in dem C5-Katalog mit den Bausteinen SSO-01 „Richtlinien und Anweisungen zur Steuerung und Überwachung Dritter“, SSO-02 „Risikobeurteilung der Dienstleister und Lieferanten“ und SSO-04 „Überwachung der Einhaltung der Anforderungen“ thematisiert. Weiterhin wird mit dem Baustein SSO-05 „Ausstiegsstrategie für den Bezug von Leistungen“ eine Definition von Ausstiegsstrategien gefordert.

Zu NIS2UmsuCG.1.6
Bei diesen Risikomanagementmaßnahmen können zum einen Lieferantenmanagement-Controls Anwendung finden, aufgrund des „Erwerbs“ der Systeme und zum Anderem können Maßnahmen zum Schwachstellenmanagement und Sicherheitsmanagement Anwendung finden. Hierunter fallen unter

anderem die Controls A.5.24 „Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen“, A.6.8 „Meldung von Informationssicherheitsereignissen“, A.8.8 „Handhabung von technischen Schwachstellen“ und A.8.20 „Sicherheit von Netzwerkdiensten“.
Für die Sicherheit in der Entwicklung kann APP.7 „Entwicklung von Individualsoftware“ Anwendung finden. Weiterhin kann zum Schwachstellenmanagement der Bausteine DER.1 „Detektion von sicherheitsrelevanten Ereignissen“ Verwendung finden, da hier auch der Umgang mit Schwachstellen, von der Erkennung bis hin zur Meldung, thematisiert werden.
Zum Thema des Schwachstellenmanagements beinhalten die Bausteine PSS-02 „Identifikation von Schwachstellen des Cloud-Dienstes“ und PSS-03 „Online-Register bekannter Schwachstellen“ Anforderungen an den Betreiber des Cloud-Dienstes.

Zu NIS2UmsuCG.1.7
Hierzu kann Kapitel 9 „Bewertung der Leistung“ herangezogen werden. Konkrete Controls lassen sich hier nicht vollumfänglich anführen. Anwendbar sind jedoch speziell A.5.35 „Unabhängige Überprüfung der Informationssicherheit“ und A.5.36 „Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit“, da diese jeweils die Thematik mit beleuchten.
Der Baustein DER.3.1 „Audits und Revisionen“ beschäftigt sich mit der Überprüfung der vorhandenen Prozesse auf Wirksamkeit und kann somit passgenau angewendet werden.
Um die Bewertung der getroffenen Maßnahmen zu beurteilen, sehen die Bausteine COM-02 „Richtlinie für die Planung und Durchführung von Audits“ und COM-03 „Interne Audits des Informationssicherheitsmanagementsystems“ konkrete Anforderungen an Audits vor. Weiterhin werden, durch den Baustein COM-04 „Informationen über die Informationssicherheitsleistung und Managementbewertung des ISMS“, Anforderungen an die oberste Leitung, bezüglich der Bewertung der Leistung des ISMS, gestellt.

Zu NIS2UmsuCG.1.8
In diesem Fall sind eine Vielzahl von Controls anwendbar, da der Begriff „Cyberhygiene“ sehr breit ausgelegt ist. Hierunter fallen unter anderem A.5.16 „Identitätsmanagement“ und A.5.18 „Zugangsrechte“. Weiterhin behandelt A.6.3 „Informatiosnsicherheitsbewusstsein, -ausbildung und -schulung“ konkret den Schulungsgedanken der geforderten Maßnahme.
Speziell zum Thema der Mitarbeiterschulungen bietet der Baustein ORP.3 „Sensibilisierung und Schulung zur Informationssicherheit“ Anforderungen zu diesem Thema.
Da „Cyberhygiene“ sehr weit gefasst ist, können hier sämtliche Bausteine, welche sich mit der Sicherheit von Informationssystemen befassen, Anwendung finden. Speziell zum Thema der Schulung bietet der Baustein HR-03 „Programm zur Sicherheitsausbildung und Sensibilisierung“ Anforderungen.

Zu NIS2UmsuCG.1.9
Im Rahmen dieser Maßnahme lässt sich passgenau die Control A.8.24 „Verwendung von Kryptographie“ anwenden, da hier konkret Regeln zum Einsatz von Kryptographie thematisiert werden.
Zum Thema der Kryptographie bietet der Baustein CON.1 „Kryptokonzept“ Anforderungen zur

Erstellung eines Konzepts zum Einsatz von Kryptographie und Verschlüsselung.
Zum Thema der Kryptographie findet sich im C5-Katalog die CRY-Reihe, welche sich ausschließlich mit Kryptokonzepten und deren Einsatz beschäftigt.

Zu NIS2UmsuCG.1.10
Da es sich hierbei hauptsächlich um den Umgang mit Anlagen handelt, greifen hier eine Vielzahl von Controls. Unter anderem können A.5.15 „Zugangssteuerung“, A.5.10 „Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten“. Weiterhin kommt, für die Personalüberprüfung, A.6.1 „Sicherheitsüberprüfung“ in Frage.
Für diese Maßnahme bietet der Baustein ORP.4 „Identitäts- und Berechtigungsmanagement“ umfangreiche Anforderungen und Informationen.

Da es sich hierbei, nach unserer Vermutung, um die Zugangskontrolle zu Anlagen handelt, findet hier unter anderem IDM-01 „Richtlinie für Zugangs- und Zugriffsberechtigung“ Anwendung. Zum Thema der Personalsicherheit ist auf Baustein HR-01 „Überprüfung der Qualifikation und Vertrauenswürdigkeit“ zu verweisen, welche sich ebenfalls mit der Integrität des Personals beschäftigt.

Zu NIS2UmsuCG.1.11
Hier können passgenau die Controls A.5.16 „Identitätsmanagement“ und A.5.17 „Informationen zur Authentifizierung“ angewendet werden, da diese sich mit der Authentifizierung beschäftigen. Weiterhin kann Control A.5.14 „Informationsübertragung“ angewendet werden, da hier die Sicherheit von Informationen, während des Transports, thematisiert wird.
Parallel zu Nummer 9 lässt sich Baustein ORP.4 „Identitäts- und Berechtigungsmanagement“ ebenfalls auf diese Maßnahme anwenden, da hier die Authentifizierung thematisiert wird.
Der C5-Katalog bietet mit der IDM-Reihe, neun Bausteine, welche sich mit der Authentifizierung beschäftigen. Weiterhin sind in den Bausteinen CRY-01 „Richtlinie zur Nutzung von Verschlüsselungsverfahren und Schlüsselverwaltung“ und CRY-02 „Verschlüsseleung von Daten bei der Übertragung (Transportverschlüsselung)“ Anforderungen an die gesicherte Kommunikation gegeben.

Zu NIS2UmsuCG.2
Die ISO 27001 bietet zum Thema „Systeme zur Angriffserkennung“ mit der Control A.8.16 „Überwachung von Aktivitäten“ eine Möglichkeit zur Konformität. Diese Control spricht von der Überwachung von Netzwerken, Systemen und Anwendungen auf anormales Verhalten. Der Zweck dieser Control ist es, anormales Verhalten und potenzielle Informationssicherheitsvorfälle zu erkennen und passt dementsprechend passgenau auf die Anforderung.
Das IT-Grundschutz-Kompendium verfügt über mehrere Bausteine und Anforderungen, um eine Konformität diesbezüglich zu erlangen. Zunächst behandelt die Anforderung DER.1.A15 „Zentrale Detektion und Echtzeitüberprüfung von Ereignismeldungen“ dies, indem sie beschreibt, dass ein zentrales System zur automatischen Ereigniserkennung existieren SOLLTE. In Verbindung mit der Umsetzung der Anforderung DER.1.A.17 „Automatische Reaktion auf sicherheitsrelevante Ereignis-

se“ erfolgt ebenfalls die vorgesehenen automatischen Beseitigungsmaßnahmen. Weiterhin SOLLTEN nach der Anforderung SYS.1.1.A27 „Hostbasierte Angriffserkennung“ Systeme, welche unter anderem dazu in der Lage sind geeignete IPS-Maßnahmen zu vollziehen. Alle genannten Anforderungen erhalten die Kategorie T, da sie nicht selbständig NIS2UmsuCG.2 erfüllen.
Der C5 Katalog behandelt dieses Thema im Baustein OPS-13. Hier wird darauf eingegangen, wie Protokollierungsdaten automatisch auf Ereignisse überwacht werden sollen und ist insofern passend für die Anforderung.

Zu NIS2UmsuCG.3
Bei der Anforderung handelt es sich elementar darum, dass ein Informationssicherheitsvorfall der zuständigen Behörde - hier das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) - binnen 24 Stunden zu melden ist.

Zu diesem Zweck hält die ISO 27001 die Control A.5.5 „Kontakt mit Behörden“ parat. Dieser adressiert passgenau die Anforderung. Er beschreibt, dass der Informationsfluss zu unter anderem Aufsichtsbehörden (hier: BBK) gewährt ist. Hierzu soll die Organisation festlegen wann und durch wen solche Vorfälle zu melden sind. Da die Control somit der Anforderung Genüge tut, wird dieser Control die Kategorie V zugewiesen.
Das IT-Grundschutz-Kompendium behandelt den Meldeprozess von Sicherheitsvorfällen innerhalb des Bausteins DER.2.1 „Behandlung von Sicherheitsvorfällen“. Die MUSS-Anforderung DER.2.1.A4 „Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen“ schreibt neben der internen Meldung auch die Meldung zu externen Stellen und Behörden vor. Die Standard-Anforderung DER.2.1.A9 Festlegung von Meldewegen für Sicherheitsvorfälle thematisiert zusätzlich, wer diese Informationen an Dritte weitergeben SOLLTE. Da durch die Umsetzung dieses Bausteines und der Baustein-Anforderungen, der gesetzlichen Anforderung Genüge getan wird, wird die Kategorie V vergeben.
Der C5-Kritierenkatalog verfügt über kein Kriterium, welches sich mit der Meldung an zuständige Behörden beschäftigt.

Zu NIS2UmsuCG.4
Da es sich bei dieser Anforderung im Kern ebenfalls um den Kontakt mit Behörden handelt, wird auf dieselbe Control zurückgegriffen wie bei NIS2UmsuCG.3.1. Diese Control schließt nicht nur den Kontakt zu Behörden bei Sicherheitsvorfällen ein, sondern spricht von der Gewährleistung des Informationsflusses allgemein und trifft somit zu. Entsprechend der vorangegangenen Erläuterung wird die Kategorie V vergeben.
Im Rahmen des IT-Grundschutz-Kompendiums kann der Baustein ORP.5 „Compliance Management (Anforderungsmangement)“ herangezogen werden. Dieser Baustein verfügt über keine spezifische Anforderung, welche konkret eine Registrierung bei zuständigen Behörden fordert. ORP.5.A1 „Identifikation der Rahmenbedingungen“ schreibt jedoch vor, dass alle rechtlichen Anforderungen erfasst werden müssen. In Verbindung mit der darauffolgenden Anforderung ORP.5.A2 „Beachtung der Rahmenbedingungen“, welche Führungskräfte zur unternehmensweiten Einhaltung der erfassten

Rahmenbedingungen verpflichtet, kann dennoch eine Konformität erlangt werden. Deshalb erhalten beide Anforderung die Kategorie T.
Der C5 Katalog schreibt mit dem Baustein COM-01 „Identifizierung anwendbarer gesetzlicher, regulatorischer, selbstauferlegter oder vertraglicher Anforderungen“ vor, dass alle zutreffenden gesetzlichen und rechtlichen Anforderungen dokumentiert werden müssen. Eine konkrete Registrierungspflicht geht aus dem C5-Katalog jedoch nicht einher. COM-01 wird dementsprechend als T kategorisiert.

Zu NIS2UmsuCG.5

Erneut kann hierzu die Control A.5.5 herangezogen werden. Diese beschreibt jedoch lediglich die Meldung des Informationssicherheitsvorfalles an Behörden und ist dementsprechend nicht auf den Kunden anwendbar, um dieser Anforderung Genüge zu tun. Passender ist zu diesem Zweck die Control A.5.26 „Reaktion auf Informationssicherheitsvorfälle“. Die ISO 27002 beschreibt zu diesem Punkt, dass die Reaktion ebenfalls eine Mitteilung *„[...] an alle relevanten internen und externen interessierten Parteien [...]“* ([DEU24b], 5.26 Anleitung e) erfolgen sollte. Da Kunden als „externe interessierte Parteien“ angesehen werden können, trifft diese Control hier zu. Beide Controls erhalten dementsprechend die Kategorie T.
Das IT-Grundschutz-Kompendium hat zur Behandlung dieser Thematik die SOLLTE-Anforderung DER.2.1.A9 „Festlegung von Meldewegen für Sicherheitsvorfällen“. Diese legt fest, dass festgelegt werden SOLLTE, wer Informationen über Sicherheitsvorfälle an Dritte weitergibt. Da dies die Kunden mit einschließt, kann mit der Umsetzung dieser Anforderung eine Konformität erlangt werden und somit erhält diese Anforderung die Kategorie T.
Die Informationspflicht bei Sicherheitsvorfällen gegenüber dem Kunden ist im C5 Katalog in der Anforderung OPS-21 „Einbindung des Cloud-Kunden bei Störungen (Incidents)“ verankert. Dieser verlangt, dass der Cloud-Kunde über den ihn betreffenden Störungen informiert und ggf. in die Behebung mit eingebunden wird. Durch die Umsetzung ist NIS2UmsuCG5 Genüge getan und die Anforderung erhält Kategorie V.

Zu NIS2UmsuCG.6.1

Bei der Erstellung der Informationssicherheitspolitik und -richtlinien, nach Control A.5.1, sollen ebenfalls gesetzliche und rechtliche Anforderungen berücksichtigt werden. Da NIS2UmsuCG.6.1 von zwingenden Maßnahmen spricht, sind diese folglich in der unternehmensinternen Informationssicherheitspolitik zu verankern. Auf dieser Basis kann im Anschluss Control A.5.4 „Verantwortlichkeiten der Leitung“ herangezogen werden, welche davon spricht sicherzustellen, dass die festgelegten Richtlinien umgesetzt und eingehalten werden. In Kombination tragen beide Controls zu der Konformität mit dieser Anforderung bei, weshalb diese beide die Kategorie T erhalten.
In der Anforderung ORP.5.A2 „Beachtung der Rahmenbedingungen“ werden Führungskräfte - also auch die Geschäftsleitungen - dazu verpflichtet rechtliche und gesetzliche Maßnahmen unternehmensweit einzuhalten. Hierdurch wird NIS2UmsuCG.6.1 Genüge getan und es wird die Kategorie V zugewiesen.
Der C5-Katalog schreibt mit der Anforderung COM-03 „Interne Audits des Informationssicher-

heitsmanagementsystems“ vor, dass mindestens einmal jährlich die Umsetzung von gesetzlichen Maßnahmen, durch qualifiziertes Personal, kontrolliert wird. Es ist davon auszugehen, dass die Geschäftsleitung dazu qualifiziert ist und insofern wird dem geforderten „Überwachen“ Genüge getan. Der Billigunsteil wird durch SP-01 „Dokumentation, Kommunikation und Bereitstellung von Richtlinien und Anweisungen“ implizit Genüge getan, indem diese Anforderung beschreibt, dass Richtlinien und Anweisungen durch die oberste Leitung genehmigt werden. Da beide Anforderungen NIS2UmsuCG.6.1 nicht selbstständig erfüllen, wird jeweils Kategorie T vergeben.

Zu NIS2UmsuCG.6.2

Schulungen werden von der ISO 27001 durch die Control A.6.3 „Informationssicherheitsbewusstsein, -ausbildung und -schulung“ adressiert. Es sollen laut dieser Control regelmäßige Schulungen stattfinden und trifft somit auf NIS2UmsuCG.6.2 zu. Eine Hürde bei der Anwendung dieser Control liegt jedoch im Sprachgebrauch der Control. Bei den Ausführungen in der ISO 27002 beschreibt die Control lediglich das Personal der Organisation. Zur passenden Anwendung ist es folglich notwendig zu definieren, ob die Geschäftsleitung ebenfalls Personal der Organisation ist oder einen anderen Status innehat. Aufgrund der vorherigen Begründung erhält diese Control jedoch die Kategorie V.
Im Gegensatz zu der ISO 27001 adressiert das IT-Grundschutz-Kompendium die Sensibilisierung und Schulung der Geschäftsleitung explizit. Dies ist in der Anforderung ORP.3.A1 „Sensibilisierung der Institutionsleitung für Informationssicherheit“ festgehalten, welche die Vorgesetzten zum Vorangehen bei Schulungsmaßnahmen verpflichtet. Entsprechend wird die Kategorie V zugewiesen.
Für den C5-Katalog gilt selbige Problematik, wie für die ISO 27001. Hier wird in Anforderung HR-03 „Programm zur Sicherheitsausbildung und Sensibilisierung“ zwar Schulungen für interne Mitarbeiter gefordert, jedoch ist selbstständig zu klären, ob die Geschäftsleitung ein Mitarbeiter ist. Es wird dennoch die Kategorie V zugewiesen.

Zu NIS2UmsuCG.7

In diesem Fall kann eine Kombination von zwei Controls Anwendung finden. Zum einen legt Control A.5.31 „Juristische, gesetzliche, regulatorische und vertragliche Anforderungen“ fest, dass gesetzliche und rechtliche Anforderungen erfasst, aktuell gehalten und ein Prozess entwickelt werden sollte, um diese zu behandeln. In Verbindung mit der Control A.5.5 „Kontakt mit Behörden“, welche einen permanenten Informationsfluss zu Aufsichtsbehörden bewerkstelligt, kann NIS2UmsuCG.7 Genüge getan werden, weshalb beide Controls folglich die Kategorie T erhalten.
Im Rahmen des IT-Grundschutz-Kompendiums kann der Baustein ORP.5 „Compliance Management (Anforderungsmanagement)“ herangezogen werden. Dieser Baustein verfügt über keine spezifische Anforderung, welche die Nachweispflicht adressiert.. ORP.5.A1 „Identifikation der Rahmenbedingungen“ schreibt jedoch vor, dass alle rechtlichen Anforderungen erfasst werden müssen. In Verbindung mit der darauffolgenden Anforderung ORP.5.A2 „Beachtung der Rahmenbedingungen“, welche Führungskräfte zur unternehmensweiten Einhaltung der erfassten Rahmenbedingungen verpflichtet, kann dennoch eine Konformität erlangt werden. Deshalb erhalten beide Anforderung die Kategorie T.
Nach der Anforderung COS-01 „Technische Schutzmaßnahmen“ hat ein Cloud-Provider Schutzmaß-

nahmen zu implementieren, welche auf Grundlage von Mustern Angriffe erkennen kann und darauf reagieren kann. Somit ist NIS2UmsuCG.7 Genüge getan und es wird Kategorie V vergeben.

4.5 BSIG Konformität

Zu BSIG.1.1

Das BSI hat zum Zwecke der Konkretisierung ein Dokument ([BUN20b]) veröffentlicht. Dieses Dokument liefert anhand von 100 Kriterien eine umfassende Konkretisierung der geforderten *angemessene organisatorische und technische Vorkehrungen*. Diese Kriterien basieren auf dem C5-Katalog. Es wird an dieser Stelle keine Erläuterung der Gedankengänge erfolgen, sondern lediglich eine Aufnahme der jeweiligen C5-Kriterien in den Katalog vorgenommen. Darüber hinaus wird eine kommentarlose Zuordnung von äquivalenten Bausteinen/Controls (IT-Grundschutz-Kompendium/ISO 27001), anhand des vorangegangenen Kapitels, durchgeführt und in den Katalog aufgenommen.

Zu BSIG.1.2

Die ISO 27001 fordert eine kontinuierliche Überwachung ihrer IKT-Systeme und Anwendungen innerhalb der Control A8.16 „Überwachung von Aktivitäten“. Bei Umsetzung dieser Control kann gewährleistet werden, dass anormales Verhalten erkannt und durch Korrekturmaßnahmen korrigiert werden kann.

Zum Zwecke des Monitorings bietet das IT-Grundschutz-Kompendium eine breite Auswahl an Anforderungen aus verschiedenen Bausteinen. Generelles IT-Monitoring wird durch die Anforderungen OPS.1.1.1.A9 „Durchführung von IT-Monitoring“ gefordert. Der Baustein DER.1 „Detektion von sicherheitsrelevanten Ereignissen“ fordert in Anforderung DER.1.A5 „Einsatz von mitgelieferten Systemfunktionen zur Detektion“, dass sämtliche nativ vorhandenen Detektionsfunktionen in IT-Systemen aktiviert sein müssen. Weiterhin wird hier durch DER.1.A6 „Kontinuierliche Überwachung und Auswertung von Protokollierungsdaten“ eine möglichst permanente Überwachung von Protokollierungsdaten. Darüber hinaus fordert beispielsweise DER.1.A15 „Zentrale Detektion und Echtzeitüberprüfung von Ereignismeldungen“ eine zentrale Komponente, welche Informationssicherheitsereignisse erkennt und automatisiert auswertet, sofern ein erhöhter Schutzbedarf besteht. Gerade mit wachsendem Schutzbedarf wird der Einsatz von automatisierter Angriffserkennung vermehrt gefordert. So ist der Einsatz von hostbasierten Angriffserkennungssystemen auch bei Servern gefordert, wenn dieser Schutzbedarf besteht (SYS.1.1.A27).

Die kontinuierliche Erkennung von Ereignissen wird von dem C5-Katalog in dem Kriterium OPS-13 „Protokollierung und Überwachung - Erkennung von Ereignissen“ behandelt. Diese fordert eine automatische Auswertung der Protokolldaten, welche zu einer Sicherheitszielverletzung führen.

Zu BSIG.1.3

Die ISO 27001 enthält keine konkrete Control, welche die Nachweiserbringung zur Erfüllung von

gesetzlichen Anforderungen fordert. Es kann sich jedoch im weiteren Sinne auf zwei Controls bezogen werden. Control A5.31 „Juristische, gesetzliche, regulatorische und vertragliche Anforderungen“ fordert, dass die Erfassung und Einhaltung von allen rechtlichen Anforderungen. Da es sich bei der Nachweiserbringung um eine solche rechtliche Anforderung handelt, muss die Erbringung, durch die Anwendung von dieser Control, erbracht werden. Gepaart mit dem, aus der Control A5.5 „Kontakt mit Behörden“, Informationsfluss, kann die Nachweiserbringung gewährleistet werden.
Das IT-Grundschutz-Kompendium widmet sich dieser Anforderung implizit durch die Anwendung des Bausteines ORP.5 „Compliance Management“. Hier fordert die Basis-Anforderungen ORP.5.A1 „Identifikation der Rahmenbedingungen“, dass gesetzliche Rahmenbedingungen identifiziert und dokumentiert werden. In Verbindung mit ORP.5.A2 „Beachtung der Rahmenbedingungen“, welche Führungskräfte dazu verpflichtet für die Einhaltung der identifizierten Rahmenbedingungen zu sorgen, kann die Nachweiserbringung gewährleistet werden.
Auch der C5-Katalog verfügt über ein Kriterium, welches der Anforderung gerecht werden kann. Das Kriterium COM-01 „Identifizierung anwendbarer gesetzlicher, regulatorischer, selbstauferlegter oder vertraglicher Anforderungen“ fordert - ähnlich wie beim IT-Grundschutz-Kompendium -, dass die gesetzlichen Anforderungen identifiziert und zusammen mit Verfahren zur Einhaltung dokumentiert werden.

5 Betrachtung der Ergebnisse

Die vorliegende Arbeit befasste sich mit der Fragestellung, inwiefern etablierte Informationssicherheitsstandards genutzt werden können, um den neuen gesetzlichen Anforderungen, im Rahmen der Sicherheitsunion 2020 bis 2025, Genüge zu tun.

Die eingehende Analyse der relevanten gesetzlichen Informationssicherheitslandschaft hat als Ergebnis acht Gesetze/Verordnungen (CER, CRA, NIS2, DORA, EUDGSVO, Kritis-DachG, NIS2UmsuCG, BSI-Gesetz) hervorgebracht. Drei von diesen acht Gesetzen (Kritis-DachG, NIS2UmsuCG, BSI-Gesetz) sind national geltende Gesetze für Deutschland. Von diesen drei Gesetzen befassen sich zwei (Kritis-DachG, NIS2UmsuCG) im Kern mit der nationalen Umsetzung der übergeordneten europäischen Verordnungen, während das dritte (BSI-Gesetz) sich eigenständig unter anderem der Informationssicherheit beschäftigt. Innerhalb dieser acht Gesetzen/Verordnungen konnten insgesamt 76 Anforderungen identifiziert werden, welche potenziell relevant für KMU sind. Dem gegenüber stehen drei etablierte Standards/Normen (ISO 27001, IT-Grundschutz-Kompendium, BSI C5). Durch die Analyse der Standards/Normen konnten insgesamt 540 Anforderungs- und Maßnahmenpaare gebildet werden.

Der erarbeitete Katalog zeigt, dass die ausgewählten Standards und Normen eine gute Basis für Handlungen zur Konformität mit den identifizierten Gesetze und Verordnungen darstellen. Vor Beginn der Arbeit davon ausgegangen, dass die Normen und Standards eine vollständige Konformität mit den einzelnen Gesetzen und Verordnungen hergestellt werden kann. Diese Erwartung wurde jedoch durch die Ausführungen in Kapitel 4 teilweise widerlegt und es ist zu beobachten, dass die gesetzlichen Anforderungen in spezifischen Fällen über die Maßnahmen der jeweiligen Standards und Normen hinausgehen.
Besonders herauszustellen ist hierbei der Cyber Resilience Act (vgl.2.1.1), welcher sich mit der Cybersicherheit von Produkten mit digitalen Elementen befasst und als schwierig, bezüglich der Erfüllung anhand der ausgewählten Standards, einzustufen ist. Die hierfür erarbeiteten Anforderungs- und Maßnahmenpaare sind als Interpretation zu betrachten, welche nicht exakt dem Normungs- bzw Standardtext übereinstimmt. Dies ist zurückzuführen auf die jeweilige Zielsetzung der Standards und Normen. Die ISO 27001 verfolgt das Ziel der Entwicklung, Implementierung und Weiterentwicklung eines ISMS. Dementsprechend wird hier ein umfassender Gesamtansatz zur Informationssicherheit etabliert, welcher jedoch im Rahmen der 2.1.1 über eine nicht ausreichende Tiefe verfügt, um die produktspezifischen Anforderungen zu genügen.

Die beste Abdeckung der Anforderungen wird mit dem IT-Grundschutz-Kompendium erzielt. Für dieses sind für die 76 Anforderungen X der 540 Paare erfasst worden. Dieses Ergebnis lässt sich auf den Umfang des IT-Grundschutz-Kompendiums zurückführen. Das Kompendium umfasst, mit seinen

über 800 Seiten, eine Vielzahl an Perspektiven zur Absicherung eines Unternehmens und es konnte in den meisten Fällen ohne Probleme mindestens eine Maßnahme zur Erfüllung der rechtlichen Anforderungen erfasst werden.
Ebenfalls der BSI C5-Kriterienkatalog verfügt ebenfalls über eine Vielzahl von Maßnahmen, welche schlussendlich zur Konformität mit den rechtlichen Anforderungen beiträgt. Besonders hervorzuheben ist, dass dieser vor allem in den nationalen Gesetzen zu einem guten Maß an Konformität beitragen kann. Defizite zeigt dieser vorwiegend bei der Umsetzung von internationalen Gesetzen/Verordnungen. Darüber hinaus ist zu erwähnen, dass der Katalog sich primär an professionelle Cloud-Anbieter richtet [1], was sich teilweise als hinderlich im Herausarbeiten der Anforderungs- und Maßnahmenpaare herausgestellt hat.

Insgesamt lässt sich jedoch sagen, dass der entstandene Katalog einen handlichen Überblick über etwaige Maßnahmen liefert, welche zu einer Konformität von den identifizierten Gesetzen und Verordnungen führen kann. Bei der Verwendung des Kataloges muss jedoch berücksichtigt werden, dass die vorliegende Arbeit keine Qualitätskontrolle anhand von Industrieexperten vornimmt. Die jeweils identifizierten Maßnahmen beruhen ausschließlich auf die vorgenommene Literaturanalyse und theoretische Annahmen, wodurch nicht sichergestellt ist, dass die Maßnahmen in der Praxis zu dem gewünschten Erfolg führen. In der Schlussbetrachtung präsentiert sich der Katalog jedoch besonders für KMU als hilfreich, wenn diese nicht über ein dediziertes Informationssicherheitsteam verfügen, aber die Konformität ohne externe Dienstleister herstellen wollen.

[1] BSI (2020): BSI - Kriterienkatalog C5, unter: https://www.bsi.bund.de/dok/7685384 [Zugriff: 21.06.2024]

6 Fazit

In dem folgenden Kapitel werden einleitend die wichtigsten Erkenntnisse der Arbeit zusammengefasst. Im Anschluss erfolgt die Beantwortung der zugrundeliegenden Fragestellungen. Abschließend werden mögliche Fortsetzungen der Arbeit thematisiert.

6.1 Erkenntnisse der Arbeit

Der Anforderungs- und Maßnahmenkatalog zeigt als Ergebnis der Arbeit, dass die ausgewählten Standards und Normen einen guten Ausgangspunkt für die Auswahl von Maßnahmen zur Konformität darstellen. Die anfängliche Erwartung, dass die jeweiligen Standards bzw. Normen eine vollumfängliche Konformität gewährleisten können, wurde jedoch widerlegt. Dies ist vermutlich auf das Ziel bzw. den Anwendungsbereich des jeweiligen Dokuments zurückzuführen. Während die gesetzlichen Anforderungen sich spezifisch in einem Segment der Informationssicherheit ansiedeln, versuchen die Standards und Normen eine ganzheitliche Absicherung zu schaffen und weisen so teilweise eine zu oberflächliche Betrachtung auf. Die Kriterien des BSI C5-Kriterienkatalog weisen die geringste Übereinstimmung mit gesetzlichen Anforderungen auf. Grund hierfür ist zweifelsfrei der eingeschränkte Anwendungsbereich, welcher sich lediglich an professionelle Cloud-Anbieter richtet und somit nicht für jede Art von Unternehmen geeignet ist. Die ISO 27001 reiht sich im Mittelfeld der drei Standards bzw. Normen ein, was auf den Zweck der Norm zurückzuführen ist. Die ISO 27001 will ein ISMS etablieren und bleibt dementsprechend auf einer oberflächlichen Betrachtung der jeweiligen Aspekte, um eine ganzheitliche Minimierung der Angriffsfläche der Organisation zu gewährleisten. Dies hat jedoch zur Folge, dass produktspezifische Anforderungen, wie im Rahmen von CRA, nur teilweise erfüllt werden können. Die beste Abdeckung weist das IT-Grundschutz-Kompendium auf, was zweifelsfrei auf den Umfang des Werkes zurückzuführen ist. Mit über 800 Seiten behandelt das Kompendium sowohl eine oberflächliche Minimierung von Risiken und Angriffsfläche, als auch tiefe technische Anforderungen, um dies zu gewährleisten.

6.2 Beantwortung der Fragestellungen

Nach der eingehenden Analyse der Gesetze bzw. Verordnungen und den Normen bzw. Standards, lassen sich die Fragestellungen wie folgt beantworten: Es wurden acht Gesetze bzw. Verordnungen identifiziert, welche der Sicherheitsunion 2020 bis 2025 zuzuordnen sind. Drei von diesen Gesetzen sind national auf Deutschland beschränkt, während die verbleibenden fünf auf europäischer Ebene Anwendung finden. Bei zwei von diesen national beschränkten Gesetzen handelt es sich um Umsetzungsgesetze der europäischen Verordnungen und das verbleibende Gesetz ist essenziell für die

Informationssicherheit in Deutschland. Der Katalog umfasst dabei 5 dieser Gesetze. Insgesamt stellen die identifizierten Gesetze bzw. Verordnungen 103 Anforderungen an die Informationssicherheit der betroffenen Organisationen, welche für KMU relevant sein können. Dem gegenüber stehen drei ausgewählte Normen und Standards. Aufgrundlage der zuvor identifizierten Anforderungen und den ausgewählten Normen und Standards, konnten 540 Anforderungs- und Maßnahmenpaare gebildet werden.

Der entstandene Katalog bietet einen somit einen handlichen Überblick über die gesetzlichen Anforderungen und bietet dabei eine Auswahl von Maßnahmen, aus etablierten Standards bzw. Normen, welche zu einer Konformität führen können.

6.3 Ausblick

Die vorliegende Arbeit hat gezeigt, dass mit der Verabschiedung der verschiedenen Gesetze bzw. Verordnungen eine Vielzahl an Anforderungen auf betroffenen Organisationen zukommen. Die gewonnenen Erkenntnisse und der resultierende Katalog werfen weiterführende Fragen auf. Zum einen kann sich eine weiterführende Arbeit mit der qualitativen Überprüfung und Beurteilung der gebildeten Anforderungs- und Maßnahmenpaaren beschäftigen, da diese in der vorliegenden Arbeit nicht vorgenommen wurde. Darüber hinaus erscheint es sinnvoll, die Effektivität der verschiedenen Informationssicherheitsstandards in unterschiedlichen branchenspezifischen Kontexten zu analysieren und zu vergleichen, um zu dem jeweiligen Kontext den effektivsten Standard zu wählen.
Beide dieser Themenvorschläge können zu einer Erhöhung der Informationssicherheit, bei KMU, beitragen.

Literaturverzeichnis

[BAI24] Baischew, D.; Gull, I.; Lundborg, M. u. a.: Strategische Bedeutung von Cloud-Diensten für die digitale Souveränität von KMU. Bad Honnef, 2024. URL: https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/Mittelstand/Downloads/WIK_Summary.pdf?__blob=publicationFile&v=1.

[BSI] BSIG: BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert worden ist. URL: https://www.gesetze-im-internet.de/bsig_2009/BSIG.pdf.

[BUN17a] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS). Hrsg. von Bundesamt für Sicherheit in der Informationstechnik. Bonn, 2017. URL: https://www.bsi.bund.de/dok/10027834.

[BUN17b] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-2: IT-Grundschutz-Methodik. Hrsg. von Bundesamt für Sicherheit in der Informationstechnik. Bonn, 2017. URL: https://www.bsi.bund.de/dok/10027846.

[BUN17c] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz. Hrsg. von Bundesamt für Sicherheit in der Informationstechnik. Bonn, 2017. URL: https://www.bsi.bund.de/dok/10027822.

[BUN20a] Bundesamt für Sicherheit in der Informationstechnik: Cloud Computing Compliance Criteria Catalogue - C5:2020: Kriterienkatalog Cloud Computing. Hrsg. von Bundesamt für Sicherheit in der Informationstechnik. Bonn, 2020. URL: https://www.bsi.bund.de/dok/13368652.

[BUN20b] Bundesamt für Sicherheit in der Informationstechnik: KRITIS und regulierte Unternehmen - § 8a Absatz 1 BSIG - Konkretisierung der KRITIS-Anforderungen: Hinweise zur Umsetzung der Kriterien des § 8a Absatz 1 BSIG für die Beurteilung der Informationssicherheit bei Betreibern Kritischer Infrastrukturen. Bonn, 2020. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/Konkretisierung_Anforderungen_Massnahmen_KRITIS.html.

[BUN22] Bundesamt für Sicherheit in der Informationstechnik: Lerneinheit 2.9: Wahl der Vorgehensweise. 14.03.2022. URL: https://www.bsi.bund.de/dok/10990410.

[BUN23a] Bundesamt für Sicherheit in der Informationstechnik: Business Continuity Management: BSI-Standard 200-4. Hrsg. von Bundesamt für Sicherheit in der Informationstechnik. Bonn, 2023. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html.

[BUN23b] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kompendium. Hrsg. von Bundesamt für Sicherheit in der Informationstechnik. Bonn, 2023. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html.

[BUN24a] Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland - Die Lage der IT-Sicherheit in Deutschland 2023. 6.03.2024. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html?nn=129410.

[BUN24b] Bundesministerium des Innern und für Heimat: Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz): NIS2UmsuCG. 18.10.2024. URL: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/nis2umsucg.html.

[BUN24c] Bundesministerium des Innern und für Heimat: Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz von Betreibern kritischer Anlagen: KRITIS-DachG. 18.10.2024. URL: https://ag.kritis.info/2023/07/18/referentenentwurf-des-bmi-kritis-dachgesetz-kritis-dachg/.

[BUNoJ] Bundesamt für Sicherheit in der Informationstechnik: Kapitel 3: Business Impact analysieren. Hrsg. von Bundesamt für Sicherheit in der Informationstechnik. Bonn, o.J. URL: https://www.bsi.bund.de/dok/6610972.

[DEU] Deutsches Institut für Normung e.V.: DIN EN ISO/IEC 27000:2020-06, Informationstechnik_-Sicherheitsverfahren_- Informationssicherheitsmanagementsysteme_- Überblick und Terminologie (ISO/IEC_27000:2018); Deutsche Fassung EN_ISO/IEC_27000:2020. Berlin. DOI: 10.31030/3144079. URL: https://dx.doi.org/10.31030/3144079.

[DEU24a] Deutsches Institut für Normung e.V.: Informationssicherheit, Cybersicherheit und Datenschutz - Informationssicherheitsmanagementsysteme - Anforderungen (ISO/IEC 27001:2022); Deutsche Fassung EN ISO/IEC 27001:2023. 1.01.2024. URL: https://dx.doi.org/10.31030/3479707.

[DEU24b] Deutsches Institut für Normung e.V.: Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Informationssicherheitsmaßnahmen (ISO/IEC 27002:2022); Deutsche Fassung EN ISO/IEC 27002:2022. 1.01.2024. URL: https://dx.doi.org/10.31030/3394753.

[EURa] Europäisches Parlament und Rat: DELEGIERTE VERORDNUNG (EU) .../... DER KOMMISSION vom 13.3.2024 zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung der Tools, Methoden, Prozesse und Richtlinien für das IKT-Risikomanagement und des vereinfachten IKTRisikomanagementrahmens: C/2024/1532. URL: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=PI_COM:C(2024)1532.

[EURb] Europäisches Parlament und Rat: Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020: COM/2022/454. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52022PC0454.

[EUR20] Europäische Kommission: COMMUNICATION FROM THE COMMISSION on the EU Security Union Strategy. Hrsg. von Europäische Kommission. 2020. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0605.

[EUR23a] Europäisches Parlament und Rat: Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie): Richtlinie (EU) 2022/2555. Hrsg. von I. Lella; M. Theocharidou; E. Tsekmezoglou u. a. 2023. URL: http://data.europa.eu/eli/dir/2022/2555/oj.

[EUR23b] Europäisches Parlament und Rat: Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates: Directive (EU) 2022/2557. Hrsg. von I. Lella; M. Theocharidou; E. Tsekmezoglou u. a. 2023. URL: http://data.europa.eu/eli/dir/2022/2557/oj.

[EUR23c] Europäisches Parlament und Rat: 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): Verordnung (EU) 2016/679. Hrsg. von I. Lella; M. Theocharidou; E. Tsekmezoglou u. a. 2023. URL: http://data.europa.eu/eli/reg/2016/679/oj.

[EUR23d] Europäisches Parlament und Rat: Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011: Verordnung (EU) 2022/2554. Hrsg. von I. Lella; M. Theocharidou; E. Tsekmezoglou u. a. 2023. URL: http://data.europa.eu/eli/reg/2022/2554/oj.

[EUR24a] Europäische Kommission: Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen: 2003/361/EG. 2.07.2024. URL: http://data.europa.eu/eli/reco/2003/361/oj.

[EUR24b] Europäisches Parlament und Rat: DELEGIERTE VERORDNUNG (EU) .../... DER KOMMISSION vom 13.3.2024 zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur

Festlegung der Kriterien für die Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen, der Wesentlichkeitsschwellen und der Einzelheiten von Meldungen schwerwiegender Vorfälle. 2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=PI_COM:C(2024)1519.

[EUR24c] Europäisches Parlament und Rat: Delegierte Verordnung (EU) 2024/1773 der Kommission vom 13. März 2024 zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Spezifizierung des detaillierten Inhalts der Leitlinie für vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden: 2024/1773. 20.7.2024. URL: http://data.europa.eu/eli/reg_del/2024/1773/oj.

[EUR24d] Europäisches Parlament und Rat: Delegierte Verordnung (EU) 2024/1774 der Kommission vom 13. März 2024 zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung der Tools, Methoden, Prozesse und Richtlinien für das IKT-Risikomanagement und des vereinfachten IKT-Risikomanagementrahmens: 2024/1774. 15.07.2024. URL: http://data.europa.eu/eli/reg_del/2024/1774/oj.

[JOR20] Jorzig, A.; Sarangi, F.: Digitalisierung im Gesundheitswesen. Berlin, Heidelberg: Springer Berlin Heidelberg, 2020. ISBN: 978-3-662-58305-0. DOI: 10.1007/978-3-662-58306-7.

[KER23] Kersten, H.; Schröder, K.-W.: ISO 27001: 2022/2023: Management der Informationssicherheit nach den aktuellen Standards. Edition <kes>. Wiesbaden und Heidelberg: Springer Vieweg, 2023. ISBN: 978-3-658-42243-1. URL: https://link.springer.com/978-3-658-42243-1.

[NAS24] Naseer Qureshi, K.; Newe, T.; Jeon, G. u. a.: Cybersecurity Vigilance and Security Engineering of Internet of Everything. Cham: Springer Nature Switzerland, 2024. ISBN: 978-3-031-45161-4. DOI: 10.1007/978-3-031-45162-1.

[RIT18] Ritter, T.; Bachmann, M.: „Cyberangriffe: Teil des Alltags?“ In: *Cybersecurity Best Practices: Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden*. Hrsg. von M. Bartsch; S. Frey. Wiesbaden: Springer Fachmedien Wiesbaden, 2018, S. 229–238. ISBN: 978-3-658-21655-9. DOI: 10.1007/978-3-658-21655-9{\textunderscore}18.

[STA24] Statista: ISO 27001 - Anzahl der gültigen Zertifikate weltweit bis 2022 | Statista. 28.05.2024. URL: https://de.statista.com/statistik/daten/studie/829313/umfrage/bestand-an-vergebenen-iso-27001-zertifikaten-weltweit/.

[VER20] Verizon: 2020 Data Breach Investigations Report. Hrsg. von C. D. Hylender; P. Langlois; A. Pinto u. a. 2020. URL: https://www.verizon.com/business/resources/reports/2020/2020-data-breach-investigations-report.pdf.

[VER24] Verizon: 2024 Data Breach Investigations Report. Hrsg. von C. D. Hylender; P. Langlois; A. Pinto u. a. 2024. URL: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf.

[VIE22] Viegas, V.; Kuyucu, O.: IT Security Controls. Berkeley, CA: Apress, 2022. ISBN: 978-1-4842-7798-0. DOI: 10.1007/978-1-4842-7799-7.

Abbildungsverzeichnis

Tabellenverzeichnis

A Liste der Anforderungen

Verordnung	Kennung	Fundstelle	Beschreibung
CER	CER.1.1	Art. 12	Kritische Einrichtungen müssen bei Bedarfsfällen, jedoch mind. alle vier Jahre, eine Risikobewertung durchführen. Dies muss erstmals nach neun Monaten erfolgen.
	CER.1.2	Art. 13 Abs. 1 (a)	Kritische Einrichtungen müssen Präventionsmaßnahmen für Sicherheitsvorfälle, zur Katastrophenvorsorge und zur Anpassung an den Klimawandel treffen.
	CER.1.3	Art. 13 Abs. 1 (b)	Kritische Einrichtungen müssen einen angemessenen Schutz der Räumlichkeiten, unter Berücksichtigung von Zäunen;Sperren;Verfahren zur Überwachung und Zugangskontrolle, gewährleisten.
	CER.1.4	Art. 13 Abs. 1 (c)	Kritische Einrichtungen müssen auf Sicherheitsvorfälle reagieren, sie abwehren und die Folgen solcher Vorfälle begrenzen können.
	CER.1.5	Art. 13 Abs. 1 (d)	Kritische Einrichtungen müssen Maßnahmen bezüglich dem BCM und zur Wiederherstellung nach Vorfällen treffen.
	CER.1.6	Art. 13 Abs. 1 (e)	Kritische Einrichtungen müssen ein angemessenes Personalsicherheitsmanagement gewährleisten. Dies betrifft u.A. Kategorienmanagement, Zugangsrechteverwaltung, Zulässigkeitsprüfungen nach Art. 14
	CER.1.7	Art. 13 Abs. 1 (f)	Kritische Einrichtungen müssen das Personal gemäß Art.13 Buchstaben a bis e, über die getroffenen Maßnahmen informieren und sie sensibilisieren.
	CER.1.8	Art. 13 Abs. 2	Kritische Einrichtungen müssen die Maßnahmen gemäß Abs. 1 in einem Resilienzplan dokumentieren.

Verordnung	Kennung	Fundstelle	Beschreibung
	CER.1.9	Art. 13 Abs. 3	Kritische Einrichtungen müssen einen Verbindungsbeauftragen zur Kommunikation mit Behörden benennen.
	CER.2.1	Art. 15	Kritische Einrichtungen müssen bei Bekanntwerden von Sicherheitsvorfällen die entsprechenden Behörden, binnen 24h, unterrichten. Nach spätestens einem Monat muss ein Schadensbericht erfolgen.
CRA	CRA.1.1	Art. 13 (1) (3)	Einführer dürfen Produkte mit digitalen Elementen nur in Verkehr bringen, wenn diese den Anforderungen aus Anhang 1 Abs. 1 genügen und wenn die vom Hersteller festgelegten Verfahren den Anforderungen aus Anhang 1 Abs. 2 genügen. Sofern von einem Produkt ein erhebliches Cybersicherheitsrisiko ausgeht, müssen der Hersteller und die Martküberwachungsbehörde informiert werden.
	CRA.1.2	Art. 13 (2)	Einführer müssen sicherstellen, dass die Hersteller ein Konformitätsverfahren gemäß Art. 24 durchgeführt haben, die technische Dokumentation durchgeführt wurde und gemäß Art. 22 ein CE-Kennzeichen angebracht wurde, bevor Sie das Produkt inverkehrbringen.
	CRA.1.3	Art. 13 (4) (5)	Einführer müssen dem Produkt ihren Namen, ihren eingetragenen Handelsnamen oder eingetragene Handelsmarke, ihre Postanschrift und ihre E-Mail-Adresse beilegen. Weiterhin muss sichergestellt werden, dass Anleitung und Informationen gemäß Anhang 2 beigefügt sind.

Verordnung	Kennung	Fundstelle	Beschreibung
	CRA.1.4	Art. 13 (6)	Einführer müssen bei Kenntnisnahme über eine Nicht-Konformität sofortige Korrekturmaßnahmen ergreifen, um eine Konformität wiedeherzustellen. Bei Feststellung einer Schwachstelle muss der Hersteller informiert werden. Wenn von dem Produkt ein erhebliches Cybersicherheitsrisiko ausgeht, muss die Marktüberwachungsbehörde informiert werden.
	CRA.1.5	Art. 13 (7) (8)	Einführer müssen zehn Jahre lang nach Inverkehrbringen die EU-Konformitätsnachweis aufbewahren und diese auf Verlangen in einer verständlichen Sprache übermitteln.
	CRA.1.6	Art. 13 (9)	Bei Bekanntwerden der Einstellung der Betriebstätigkeit des Herstellers, muss der Einführer unmittelbar die Marktüberwachungsbehörde und - soweit möglich - die Nutzer des Produktes informieren.
	CRA.2.1	Art. 14 (2)	Vor Bereitstellung des Produktes mit digitalen Elementen muss der Händler sicherstellen, dass das Produkt eine CE-Kennzeichnung hat und, dass Hersteller und Einführer den gestellten Anforderungen genügen.
	CRA.2.2	Art. 14 (4)	Händler müssen bei Kenntnisnahme über eine Nicht-Konformität sicherstellen, dass Korrekturmaßnahmen ergriffen werden, um eine Konformität wiederherzustellen. Bei Feststellung einer Schwachstelle muss der Hersteller und die Marktüberwachungsbehörde informiert werden.
	CRA.2.3	Art. 14 (5)	Händler müssen den EU-Konformitätsnachweis, auf Verlangen, in einer verständlichen Sprache der Marktüberwachungsbehörde übermitteln.

Verordnung	Kennung	Fundstelle	Beschreibung
	CRA.2.4	Art. 14 (6)	Bei Bekanntwerden der Einstellung der Betriebstätigkeit des Herstellers, muss der Händler unmittelbar die Marktüberwachungsbehörde und - soweit möglich - die Nutzer des Produktes informieren.
NIS2	NIS2.1.1	Art. 21 Abs. 2 (a)	Eine betroffene Entität muss ein Konzept für die Risikoanalyse und Sicherheit für Informationssysteme zu gewährleisten.
	NIS2.1.2	Art. 21 Abs. 2 (b)	Betroffene Entitäten müssen Maßnahmen zur Prävention, Detektion und Bewältigung von Informationssicherheitsvorfällen ergreifen.
	NIS2.1.3	Art. 21 Abs. 2 (c)	Betroffene Entitäten müssen Maßnahmen zur Aufrechterhaltung des Betriebs, nach einem Vorfall, und für Krisenmanagement, ergreifen.
	NIS2.1.4	Art. 21 Abs. 2 (d)	Betroffene Entitäten müssen Maßnahmen ergreifen, welche die Sicherheit in der Lieferkette gewährleisten.
	NIS2.1.5	Art. 21 Abs. 2 (e)	Betroffene Entitäten müssen Maßnahmen ergreifen, welche die Sicherheit in der Beschaffung von Netzwerk- und IT-Systemen gewährleisten und Schwachstellenmanagement, inlusive Offenlegung von Schwachstellen, betreiben.
	NIS2.1.6	Art. 21 Abs. 2 (f)	Betroffene Entitäten müssen Maßnahmen, zur Bewertung des Risikomanagements, ergreifen.
	NIS2.1.7	Art. 21 Abs. 2 (g)	Betroffene Entitäten müssen Maßnahmen ergreifen, um grundlegende Cyberhygiene und Schulungen zu gewährleisten.
	NIS2.1.8	Art. 21 Abs. 2 (h)	Betroffene Entitäten müssen Maßnahmen, zum Einsatz von Kryptografie und ggf. Verschlüsselung, ergreifen.
	NIS2.1.9	Art. 21 Abs. 2 (i)	Betroffene Entitäten müssen Maßnahmen ergreifen, um die Sicherheit des Personals und die Sicherheit von Anlagen, inklusive Zugangskontrollmanagement, zu gewährleisten.

Verordnung	Kennung	Fundstelle	Beschreibung
	NIS2.1.10	Art. 21 Abs. 2 (j)	Betroffene Entitäten müssen Maßnahmen für die Multi-Faktor- und kontinuierliche Authentifizierung ergreifen. Weiterhin müssen Sprach-, Video-, Text- und ggf. Notfallskommunikationssysteme, gesichert sein.
	NIS2.2.1	Art. 23	Betroffene Entitäten müssen die nationale Cybersicherheitsbehörde über erhebliche Störungen, Vorfälle und Bedrohungen, ihrer kritischen Dienstleistung, unmittelbar unterrichten. Zudem müssen die Empfänger jener kritischen Dienstleistung unterrichtet werden, sofern möglich.
	NIS2.2.2	Art. 27	Betroffene Entitäten müssen bis zum 17. Januar 2025 der nationalen Cybersicherheitsbehörde Daten zur Registrierung der Einrichtung übermitteln.
	NIS2.2.3	Art. 29 (2)	Betroffene Entitäten müssen sich unterneinander über Cyberbedrohungen, Beinahe-Vorfälle, Techniken und Verfahren, Kompromittierungsindikatoren etc. austauschen.
DORA	DORA.1.1	Art, 5 (2b)	Das Leitungsorgan führt Leitlinien zu der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeiten von Daten ein.
	DORA.1.2	Art.5 (1)	Finanzunternehmen verfügen über einen internen Governance- und Kontrollrahmen, um ein hohes Niveau an digitaler operationaler Resilienz zu erreichen.
	DORA.1.3	Art.5 (2)	Das Leitungsorgan muss die Umsetzung von Maßnahmen billigen und fördern.
	DORA.1.4	Art.5 (3)	Finanzunternehmen, welche keine Kleinstunternehmen sind, haben eine Funktion zur Kommunikation und Überwachung von IKT-Drittdienstleistern einzurichten.

Verordnung	Kennung	Fundstelle	Beschreibung
	DORA.1.5	Art.5 (4)	Mitglieder des Leitungsorgans müssen sich regelmäßig Schulungen unterziehen, um auf dem aktuellen Stand der Technik, im Bezug auf IKT-Risiken, zu bleiben.
	DORA.1.6	Art.6 (1-2)	Finanzunternehmen müssen über einen IKT-Risikomanagementrahmen verfügen, welcher mindestens Strategien, Leit- und Richtlinien, Verfahren sowie IKT-Protokolle und -Tools festlegt.
	DORA.1.7	Art.6 (4)	Finanzunternehmen richten eine unabhängige Kontrollfunktion, zur Überwachung des IKT-Risikos, ein.
	DORA.1.8	Art.6 (5-7)	Finanzunternehmen führen mindestens einmal jährlich, oder nach schwerwiegenden IKT-bezogenen Vorfällen und nach aufsichtsrechtlichen Anweisungen, Audits bzw. Revisionen des IKT-Risikomangementrahmen durch und verbessern diesen auf dieser Grundlage.
	DORA.1.9	Art.6 (8)	Der IKT-Risikomanagmentrahmen umfasst eine Strategie für die digitale operationale Resilienz.
	DORA.1.10	Art.13 (2-4)	Finanzunternehmen führen nach schwerwiegenden IKT-bezogenen Vorfällen eine Prüfung durch, um Ursachen und Verbesserungen für IKT-Prozesse zu ermitteln und integrieren diese Erkenntnisse in ihren IKT-Risikomanagementprozess.
	DORA.1.11	Art.13 (6)	Finanzunternehmen entwickeln Programme zur Mitarbeitersensibilisierung- und schulung.
	DORA.2.1	Art.7	Finanzunternehmen verwenden für ihr IKT-Risikomanagement IKT-Systeme, -Protokolle und -Tools, welche stets auf dem neuesten Stand der Technik sind.

Verordnung	Kennung	Fundstelle	Beschreibung
	DORA.2.2	Art.8 (1)	Finanzunternehmen klassifizieren alle IKT-gestützten Unternehmensfunktionen, Rollen und Verwantwortlichkeiten und Informations- und IKT-Assets, welche diese Funktion unterstützen.
	DORA.2.3	Art.8 (2)	Finanzunternehmen überprüfen kontinuierlich alle auf sie zutreffenden IKT-Risiken und bewerten Cyberbedrohungen und IKT-Schwachstellen.
	DORA.2.4	Art.8 (3)	Finanzunternehmen führen bei jeder wesentlichen Änderung in der Netzwerk- und Informationssysteminfrastruktur, der Prozesse oder Verfahren, eine Risikobewertung durch.
	DORA.2.5	Art.8 (5)	Finanzunternehmen erfassen alle Prozesse, welche von IKT-Drittdienstleistern abhängen und ermitteln Vernetzungen mit jenen, welche kritische oder wichtige Funktionen bereitstellen oder diese unterstützen.
	DORA.2.6	Art.9 (1)	Finanzunternehmen überwachen und kontrollieren ihre IKT-Systeme und -Tools kontinuierlich, um einen Schutz zu gewährleisten.
	DORA.2.7.1	Art.9 (4) a)	Finanzunternehmen erarbeiten und dokumentieren eine Informationssicherheitsleitlinie.
	DORA.2.7.2	Art.9 (4) b)	Finanzunternehmen richten eine solide Struktur für Netzwerk- und Infrastrukturmanagment, unter Verwendung angemessener Techniken, Methoden und Protokolle, ein.
	DORA.2.7.3	Art.9 (4) c)	Finanzunternehmen implementieren Richtlinien zum physischen und logischen Zugang zu Assets.
	DORA.2.7.4	Art.9 (4) d)	Finanzunternehmen implementieren Konzepte und Protokolle für starke Authentisierungsmechanismen und Schutzmaßnahmen für dessen kryptografische Schlüssel.

Verordnung	Kennung	Fundstelle	Beschreibung
	DORA.2.7.5	Art.9 (4) e)	Finanzunternehmen implementieren und dokumentieren Richtlinien, Verfahren und Kontrollen für ein risikoorientertes IKT-Änderungsmanagement.
	DORA.2.7.6	Art.9 (4) f)	Finanzunternehmen besitzen angemessen dokumentierte Richtlinien für Patch- und Update-Management.
	DORA.2.8	Art.10	Finanzunternehmen verfügen über Mechanismen zur Erkennung von Vorfällen.
	DORA.2.9	Art.11	Finanzunternehmen betreiben BCM. Hierzu implementieren Sie IKT-Reaktions- und Wiederherstellungspläne, auch im Bezug auf IKT-Drittdienstleister, auf Grundlage einer BIA. Die resultierenden Pläne sind regelmäßigen Audits und Revisionen zu unterziehen. Finanzunternehmen, welche keine Kleinstunternehmen sind, etablieren eine dedizierte Krisenmanagementfunktion und melden die geschätzten jährlichen Kosten, welche auf IKT-Vorfälle zurückzuführen sind.
	DORA.2.10	Art.12	Finanzunternehmen erstellen und dokumentieren Richtlinien und Verfahren zur Datensicherung, Wiedergewinnungs- und Wiederherstellungsverfahren und -methoden, welche regelmäßig getestet werden. Auf dieser Grundlage richten sie ein Datensicherungssystem ein. Datenwiedergewinnung muss dabei auf einem physisch, sowie logisch getrennten System erfolgen. Darüber hinaus müssen redundante Systeme, mit ausreichend technischen Ressourcen und Funktionen, gewährleistet werden.
	DORA.2.11	Art.17 (1)	Finanzunternehmen implementieren einen Prozess zur Erkennung, Behandlung und Meldung von IKT-bezogenen Vorfällen .

Verordnung	Kennung	Fundstelle	Beschreibung
	DORA.2.12	Art.18 (1) (2)	Finanzunternehmen klassifizieren IKT-bezogene Vorfälle und Cyberbedrohungen anhand ihrer Kritikalitätsstufe.
	DORA.2.13	Art.19	Finanzunternehmen melden schwerwiegende IKT-Vorfälle der zuständigen Behörde und unterrichten den Kunden über den Vorfall und getroffene Maßnahmen.
	DORA.2.14.1	Art.24	Finanzunternehmen, die keine Kleinstunternehmen sind, verfügen über ein umfassenden Rahmen zur Test ihrer digitalen operationalen Resilienz. Tests sind dabei mindestens einmal jährlich, durch unabhängige Parteien, durchzuführen. Der Umgang mit den resultierenden Erkenntnissen werden in Verfahren und Leitlinien festgelegt.
	DORA.2.14.2	Art.26	Finanzunternehmen, welche durch die zuständigen Behörden dazu verplfichtet wurden, führen alle drei Jahre erweiterte TLPT durch.
	DORA.2.15	Art.28	Finanzunternehmen managen das IKT-Drittparteienrisiko im Rahmen ihres IKT-Risikomanagementrahmens. Hierzu existiert ein Informationsregister, welches die vertraglichen Vereinbarungen aufführt. Darüber hinaus ist vor vertraglicher Verinabrung zu überprüfen, ob kritische oder wichtige Funktionen betroffen sind, aufsichtsrechtliche Bedingungen erfüllt sind und alle Risiken ermittelt und bewertet sind.
	KRITIS-DachG.1	Art.6 (1)	Betreiber kritischer Anlagen müssen sich spätestens drei Monate nach Geltung als Betreiber kritscher Anlagen beim BBK registrieren.
	KRITIS-DachG.2	Art.9 (1)	Betreiber kritischer Anlagen führen mindestens alle vier Jahre eine Risikoanalyse und Risikobewertung, auf Grundlage der nationalen Risikoanalyse und -bewertung, durch.

Verordnung	Kennung	Fundstelle	Beschreibung
	KRITIS-DachG.3.1.1	Art.10 (1) 1. & (3)	Betreiber kritischer Anlagen müssen nach Ablauf von zehn Monaten Maßnahmen ergreifen, um das Vorfallsauftreten zu verhindern. Hierzu gehören u.A. Notfallversorgungsmaßnahmen und Maßnahmen zur Anpassung an den Klimawandel.
	KRITIS-DachG.3.1.2	Art.10 (1) 2. & (3)	Betreiber kritischer Anlagen müssen nach Ablauf von zehn Monaten Maßnahmen ergreifen, um Schutz für ihre Liegenschaft und Anlagen zu gewährleisten. Hierzu gehören u.A. Objektschutz, Überwachung der Umgebung, Detektionsgeräte und Zugangskontrollen.
	KRITIS-DachG.3.1.3	Art.10 (1) 3. & (3)	Betreiber kritischer Anlagen müssen nach Ablauf von zehn Monaten Maßnahmen ergreifen, um angemessen auf Vorfälle reagieren, sie abzuwehren und Schadensbegrenzung betreiben zu können. Hierzu gehören u.A. Risiko- und Krisenmanagementverfahren, Ablaufprotokolle für Alarmfälle.
	KRITIS-DachG.3.1.4	Art.10 (1) 4. & (3)	Betreiber kritischer Anlagen müssen nach Ablauf von zehn Monaten Maßnahmen ergreifen, um die kritische Dienstleistung wiederherstellen zu können. Hierzu gehört u.A. Maßnahmen zum Aufrechterhalten des Betriebs und Ermittlung alternativer Lieferketten.
	KRITIS-DachG.3.1.5	Art.10 (1) 5. & (3)	Betreiber kritischer Anlagen müssen nach Ablauf von zehn Monaten Maßnahmen ergreifen, um Personalsicherheitsmanagement betreiben zu können. Hierzu gehören u.A. Festlegung von Personalkategorien, Zugangsrechteverwaltung, Qualifikationsfestlegung und Zuverlässigkeitsprüfungen.

Verordnung	Kennung	Fundstelle	Beschreibung
	KRITIS-DachG.3.1.6	Art.10 (1) 6. & (3)	Betreiber kritischer Anlagen müssen nach Ablauf von zehn Monaten Maßnahmen ergreifen, um Personal angemessen zu schulen. Hierzu gehören u.A. Schulungen, Bereitstellen von Informationsmaterial und Übungen.
	KRITIS-DachG.3.2	Art.10 (9)	Betreiber kritischer Anlagen müssen einen Resilienzplan erstellen, in dem die gewählten Maßnahmen und die Umsetzung festgehalten ist.
	KRITIS-DachG.4	Art.11 (1)	Betreiber kritischer Anlagen müssen auf Weisung der zuständigen Behörde (BBK) einen Nachweis über die Einhaltung der geforderten Maßnahmen nach §10 Abs. 1 erbringen.
	KRITIS-DachG.5	Art.12 (1)(3)	Betreiber kritischer Anlagen melden Vorfälle, welche die Erbringung der kritischen Dienstleistung erheblich stören oder stören könnte dem BBK. Die erste Meldung muss innerhalb 24 Stunden nach Kenntnis erfolgen und spätestens nach innerhalb eines Monats erfolgt ein ausführlicher Bericht bezüglich des Vorfalls.
	KRITIS-DachG.6.1	Art.14 (1)	Geschäftsleiter von Betreibern kritischer Anlagen müssen die ergriffenen Maßnahmen nach §10 Abs. 1 überwachen, billigen und unterstützen.
	KRITIS-DachG.6.2	Art.14 (2)	Geschäftsleiter von Betreibern kritischer Anlagen müssen sich regelmäßigen Schulungen unterziehen, um ihre Kenntnisse und Fähigkeiten auf neuen Stand zu bringen.
NIS2UmsuCG	NIS2UmsuCG.1.1	Art. 30 (1)	Besonders wichtige und wichtige Einrichtungen müssen die Umsetzung der gewählten Maßnahmen dokumentieren.
	NIS2UmsuCG.1.2	Art.30 (2) 1	Besonders wichtige und wichtige Einrichtungen müssen Maßnahmen ergreifen, um ein Konzept für die Risikoanalyse und Sicherheit für Informationssysteme zu gewährleisten.

Verordnung	Kennung	Fundstelle	Beschreibung
	NIS2UmsuCG.1.3	Art.30 (2) 2	Besonders wichtige und wichtige Einrichtungen müssen Maßnahmen zur Bewältigung von Informationssicherheitsvorfällen ergreifen.
	NIS2UmsuCG.1.4	Art.30 (2) 3	Besonders wichtige und wichtige Einrichtungen müssen Maßnahmen zur Aufrechterhaltung des Betriebs nach einem Vorfall und für Krisenmanagement ergreifen.
	NIS2UmsuCG.1.5	Art.30 (2) 4	Besonders wichtige und wichtige Einrichtungen müssen Maßnahmen ergreifen, welche die Sicherheit in der Lieferkette gewährleisten.
	NIS2UmsuCG.1.6	Art.30 (2) 5	Besonders wichtige und wichtige Einrichtungen müssen Maßnahmen ergreifen, welche die Sicherheit in der Beschaffung von Netzwerk- und IT-Systemen gewährleisten und Schwachstellenmanagement, inklusive Offenlegung von Schwachstellen, betreiben.
	NIS2UmsuCG.1.7	Art.30 (2) 6	Besonders wichtige und wichtige Einrichtungen müssen Maßnahmen ergreifen, um das Risikomanagement bewerten zu können.
	NIS2UmsuCG.1.8	Art.30 (2) 7	Besonders wichtige und wichtige Einrichtungen müssen Maßnahmen ergreifen, um grundlegende Cyberhygiene und Schulungen zu gewährleisten.
	NIS2UmsuCG.1.9	Art.30 (2) 8	Besonders wichtige und wichtige Einrichtungen müssen Maßnahmen, zum Einsatz von Kryptografie und ggf. Verschlüsselung, ergreifen.
	NIS2UmsuCG.1.10	Art.30 (2) 9	Besonders wichtige und wichtige Einrichtungen müssen Maßnahmen ergreifen, um die Sicherheit des Personals und die Sicherheit von Anlagen, inklusive Zugangskontrollmanagement, zu gewährleisten.

Verordnung	Kennung	Fundstelle	Beschreibung
	NIS2UmsuCG.1.11	Art.30 (2) 10	Besonders wichtige und wichtige Einrichtungen müssen Maßnahmen für die Multi-Faktor- und kontinuierliche Authentifizierung ergreifen. Weiterhin müssen Sprach-, Video-, Text- und ggf. Notfallskommunikationssysteme gesichert sein.
	NIS2UmsuCG.1.12	Art.30 (6)	Besonders wichtige und wichtige Einrichtungen müssen sicherstellen, dass bestimmte - noch nicht festgelegte - IKT-Produkte, IKT-Dienste und IKT-Prozesse nur verwendet werden, wenn diese über eine Cybersicherheitszertifizierung verfügen.
	NIS2UmsuCG.2	Art.31 (2)	Betreiber kritischer Anlagen müssen Systeme zur Angriffserkennung verwenden.
	NIS2UmsuCG.3.1	Art.32 (1) 1	Besonders wichtige und wichtige Einrichtungen müssen dem BBK nach Kenntnisnahme, spätestens nach 24 Stunden, einen erheblichen Sicherheitsvorfall melden und angeben, ob dieser grenzübergreifend ist oder auf rechtswidrige/böswillige Handlungen zurückzuführen ist.
	NIS2UmsuCG.3.2	Art.32 (1) 2	Besonders wichtige und wichtige Einrichtungen müssen dem BBK nach Kenntnisnahme, spätestens nach 72 Stunden, eines erheblichen Sicherheitsvorfalls eine Bestätigung oder Aktualisierung übermitteln. Diese beinhaltet Schweregrad und Auswirkung des Vorfalls, sowie Kompromittierungsindikatoren.
	NIS2UmsuCG.3.3	Art.32 (1) 4	Besonders wichtige und wichtige Einrichtungen müssen spätestens nach einem Monat eine Abschlussmeldung an das BBK übermitteln. Diese beinhaltet eine ausführliche Beschreibung des Sicherheitsvorfalls, Angaben zur Art der Bedrohung und Ursache, Angaben zu den Abhilfemaßnahmen, ggf. die grenzübergreifende Auswirkungen.

Verordnung	Kennung	Fundstelle	Beschreibung
	NIS2UmsuCG.3.4	Art.32 (4)	Betreiber kritischer Anlagen müssen zusätzlich die Art der betroffenen Anlage und den kritischen Dienst angeben, welcher von dem Sicherheitsvorfall betroffen ist.
	NIS2UmsuCG.4	Art.33 (1)	Besonders wichtige und wichtige Einrichtungen sind verpflichtet sich spätestens nach drei Monate nach Betriebsaufnahme bei der gemeinsamen Meldestelle des BBK und BSI zu registrieren.
	NIS2UmsuCG.5	Art.35 (2)	Einrichtungen nach Abs. 1 aus den Sektoren Finanz- und Versicherungswesen, Informationstechnik und Telekommunikation, Verwaltung von IKT-Diensten und digitale Dienste müssen den betroffenen Empfängern und dem BBK unverzüglich über die Cyberbedrohung informieren und stets über alle Maßnahmen unterrichten, die die Empfänger treffen können.
	NIS2UmsuCG.6.1	Art.38 (1)	Geschäftsleitungen von besonders wichtigen und wichtigen Einrichtungen sind verpflichtet, die Erfüllung der Maßnahmen nach §30 zu billigen und die Umsetzung zu überwachen.
	NIS2UmsuCG.6.2	Art.38 (3)	Geschäftsleitungen von besonders wichtigen und wichtigen Einrichtungen sind verpflichtet, sich regelmäßigen Schulungen zu unterziehen, um ausreichende Kenntnisse und Fähigkeiten aufrecht zu erhalten.
	NIS2UmsuCG.7	Art.39 (1)	Betreiber kritischer Anlagen müssen dem BSI alle drei Jahre Nachweise über die Einhaltung der Maßnahmen nach §30 (1) und §30 (2) erbringen.
BSIG	BSIG.1.1	Art.8a (1)	Betreiber kritischer Infrastrukturen sind verpflichtet, bis zum ersten Werktag angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, zu treffen.

Verordnung	Kennung	Fundstelle	Beschreibung
	BSIG.1.2	Art.8a (1a)	Betreiber kritischer Anlagen müssen Systeme zur Angriffserkennung einsetzen.
	BSIG.1.3	Art.8a (3)	Betreiber kritischer Anlagen müssen die Erfüllung der Anforderungen nach 1 und 1a spätestens zwei Jahre nach Inbetriebnahme und anschließend alle zwei Jahre dem BSI nachweisen.

Tabelle A.1: Mindestanforderungen
(nach Gesetzen gruppiert)

B Anforderungs- und Maßnahmenkatalog

Kennung	ISO 27001	IT-Grundschutz-Kompendium	C5-Katalog
CRA.1.1	A5.5, A5.19, A5.31, A5.36	ORP.5.A1, ORP.5.A2, OPS.2.3.A4	COM-01, COM-03, SSO-01, SSO-04, OIS-05
CRA.1.2	A5.31, A5.36	ORP.5.A1, ORP.5.A2	SP-01, COM-03
CRA.1.3	A.5.19	ORP.5.A1, ORP.5.A2	BC-01
CRA.1.4	A5.31, A5.36, A5.6, A5.5	ORP.5.A1, ORP.5.A2, DER.2.1.A4	COM-01, COM-03, SSO-01, SSO-04, OIS-05
CRA.1.5	A5.33, A5.5	OPS.1.2.2	COM-01
CRA.1.6	A5.5	ORP.5.A1 ORP.5.A2	COM-01
CRA.2.1	A5.19, A5.31, A5.36	ORP.5.A1, ORP.5.A2, OPS.2.3.A4	COM-01, COM-03, SSO-01, SSO-04, OIS-05
CRA.2.2	A5.31, A5.36, A5.6, A5.5	ORP.5.A1, ORP.5.A2, DER.2.1.A4	COM-01, COM-03, SSO-01, SSO-04, OIS-05
CRA.2.3	A5.33, A5.5	OPS.1.2.2	COM-01
CRA.2.4	A5.5	ORP.5.A1 ORP.5.A2	COM-01
DORA.1.1	A5.1	ISMS.1.A3	SP-01
DORA.1.2	-	-	-
DORA.1.3	A5.4	ORP.5.A2	COM-03, SP-01

Kennung	ISO 27001	IT-Grundschutz-Kompendium	C5-Katalog
DORA.1.4	A5.2, A5.19	ISMS.1.A6, ORP.1.A2	SSO-01, SSO-04
DORA.1.5	A6.3, A5.4	ORP.3.A1, ORP.3.A4	HR-03
DORA.1.6	A5.1, A5.2, A5.4	ISMS.1.A3, ORP.1.A1	OIS-02, OIS-06, AM-02, PS-01, PS-04, OPS-04, OPS-10, OPS-11, OPS-18, IDM-01, CRY-01, COS-08, DEV-01, DEV-03, SSO-01, SIM-01, BCM-02, COM-02
DORA.1.7	A5.2, A5.3	ISMS.1.A6, ORP.1.A2, ORP.1.A4	OIS-01, OIS-04
DORA.1.8	A5.31, A5.35	ISMS.1.A11, DER.3.1.A2, DER.3.1.A4, DER.3.1.A13, DER.3.1.A23, DER.3.1.A24, DER.3.1.A25, DER.3.1.A5	COM-01, COM-02, COM-03, COM-04, SP-02
DORA.1.9	-	-	-
DORA.1.10	A5.27	DER.2.1.A17, DER.2.1.A18	SIM-02 SIM-05
DORA.1.11	A6.3	ORP.3.A4, ORP.3.A6, ORP.3.A7, ORP.3.A9	HR-03
DORA.2.1	-	-	-
DORA.2.2	A5.9, A5.12	ORP.1.A2, ORP.1.A8, OPS.1.1.1.A6	AM-01, OIS-01

Kennung	ISO 27001	IT-Grundschutz-Kompendium	C5-Katalog
DORA.2.3	A8.8	DER.1.A12, OPS.1.1.1.A10, OPS.1.1.1.A20, OPS.1.1.1.A22, OPS.1.1.1.A23	PSS-02, PSS-03
DORA.2.4	A5.9	ORP.1.A8, OPS.1.1.1.A6	AM-01, AM-02
DORA.2.5	A5.19, A5.21	OPS.2.3.A1, ORP.1.A1	SSO-02, SSO-03, SSO-04
DORA.2.6	A8.16	OPS.1.1.1.A9, DER.1.A5, DER.1.A6, DER.1.A15, SYS.1.1.A27	OPS-13
DORA.2.7.1	A5.1	ISMS.1.A3	OIS-02
DORA.2.7.2	A8.9, A8.20, A8.21, A8.22	OPS.1.1.1.A5, NET.3.1, NET.3.1.A1	COS-01, COS-02, COS-03, COS-04, COS-05, COS-06, COS-07,
DORA.2.7.3	A5.15, A5.18, A8.3, A8.2, A8.4	ORP.4.A2 ORP.4.A5 ORP.4.A6 ORP.4.A7 ORP.4.A16	IDM-09
DORA.2.7.4	A5.16, A5.17, A8.5	ORP.4.A9 ORP.4.A12 ORP.4.A13 ORP.4.A18 ORP.4.A21	PSS-05 PSS-06 IDM-08 IDM-09
DORA.2.7.5	A8.32	OPS.1.1.3.A1 OPS.1.1.3.A5 OPS.1.1.3.A6 OPS.1.1.3.A7	DEV-03 DEV-05
DORA.2.7.6	A8.8, A8.9, A8.32	OPS.1.1.3.A1 OPS.1.1.3.A3 OPS.1.1.3.A15 OPS.1.1.3.A7 OPS.1.1.3.A8	DEV-03 DEV-05 PSS-03

Kennung	ISO 27001	IT-Grundschutz-Kompendium	C5-Katalog
DORA.2.8	A8.16	OPS.1.1.1.A9 DER.1.A5 DER.1.A6 DER.1.A9 DER.1.A15 DER.1.A16 SYS.1.1.A27	OPS-02 OPS-10 OPS-13
DORA.2.9	A5.29, A5.30	DER.4.A1	BCM-01 BCM-02 BCM-03 BCM-04
DORA.2.10	A8.13, A8.14	CON.3.A1 CON.3.A2 CON.3.A4 CON.3.A15	OPS-06 OPS-07 OPS-08 OPS-09 PS-02
DORA.2.11	A5.24, A5.25, A5.26, A5.27, A5.28, A6.8	OPS.1.1.1.A9 DER.1.A3 DER.1.A5 DER.1.A6 DER.1.A9 DER.1.A15 DER.1.A16 SYS.1.1.A27 DER.2.1.A3 DER.2.1.A9 DER.2.1.A4 DER.2.1.A2 DER.2.1.A7 DER.2.1.A10 DER.2.1.A17	SIM-01, SIM-02, SIM-03, SIM-05
DORA.2.12	A5.25	DER.2.1.A11	SIM-01 SIM-02
DORA.2.13	A5.25	DER.2.1.A4	SIM-02 SIM-05
DORA.2.14.1	A5.25	OPS.1.1.1.A22 OPS.1.1.1.A23	OPS-19
DORA.2.14.2	-	OPS.1.1.1.A23	OPS-19
DORA.2.15	A5.19, A5.20, A5.21, A5.22, A5.23	OPS.2.3	SSO-01, SSO-02, SSO-03, SSO-04, SSO-05

Kennung	ISO 27001	IT-Grundschutz-Kompendium	C5-Katalog
KRITIS-DachG.1	A5.5	ORP.5.A1, ORP.5.A2	OIS-05
KRITIS-DachG.2	-	-	OIS-06
KRITIS-DachG.3.1.1	A7.5	-	-
KRITIS-DachG.3.1.2	A7.1, A7.2, A7.3, A7.4, A7.5, A7.8	INF.1	PSS-03, PSS-04
KRITIS-DachG.3.1.3	A5.26, A5.29, A5.30	DER.2.1, DER.2.3, DER.4	SIM-01, SIM-02, SIM-03
KRITIS-DachG.3.1.4	A5.29, A5.30	DER.4	BCM-01, BCM-02, BCM-03, BCM-04,
KRITIS-DachG.3.1.5	A.5.18, A.6.1, A8.3	ORP.4.A1, ORP.4.A4, ORP.4.A6, ORP.4.A7, ORP.2.A7, ORP.2.A13	IDM-01, HR-01
KRITIS-DachG.3.1.6	A6.3	ORP.3.A3, ORP.3.A4, ORP.3.A6	HR-03
KRITIS-DachG.3.2	A5.1	ISMS.1	SP-01
KRITIS-DachG.4	A5.5, A5.31	ORP.5.A1, ORP.5.A2	COM-01
KRITIS-DachG.5	A5.5, A5.24	DER.2.1.A4, DER.2.1.A9	COM-01
KRITIS-DachG.6.1	A.5.4	ORP.5.A2	COM-03, SP-01
KRITIS-DachG.6.2	A6.3	ORP.3.A1	HR-03
NIS2UmsuCG.1.1	tbd	tbd	tbd
NIS2UmsuCG.1.2	A5.1	ISMS.1	OIS-02, SP-01, SP-02
NIS2UmsuCG.1.3	A5.24, A5.25, A5.26, A5.27, A5.28	DER.2.1, DER.2.3	SIM-01, SIM-02, SIM-03, SIM-04, SIM-05

Kennung	ISO 27001	IT-Grundschutz-Kompendium	C5-Katalog
NIS2UmsuCG.1.4	A5.29, A5.30, A8.13, A8.14	DER.4	BCM-01, BCM-02, BCM-03, BCM-04
NIS2UmsuCG.1.5	A5.19	OPS.2.3	SSO-01, SSO-02, SSO-04, SSO-05
NIS2UmsuCG.1.6	A5.24, A6.8, A8.8, A8.20	APP.7, DER.1	PSS-02, PSS-03
NIS2UmsuCG.1.7	A5.35, A5.36	DER.3.1	COM-02, COM-03, COM-04
NIS2UmsuCG.1.8	A5.16, A5.18, A6.3	ORP.3	HR-03
NIS2UmsuCG.1.9	A8.24	CON-01	CRY-01, CRY-02, CRY-03, CRY-04
NIS2UmsuCG.1.10	A5.10, A5.15, A6.1	ORP.4	IDM-01, HR-01
NIS2UmsuCG.1.11	A5.14, A5.16, A5.17	ORP.5	CRY-01, CRY-02
NIS2UmsuCG.2	A8.16	DER.1.A15, DER.1.A17, SYS.1.1.A27	OPS.13
NIS2UmsuCG.3	A5.5	DER.2.1.A4, DER.2.1.A9	Placeholder
NIS2UmsuCG.4	A5.5	DER.2.1.A4, DER.2.1.A9	Placeholder
NIS2UmsuCG.5	A5.5, A5.26	DER.2.1.A9	OPS-21
NIS2UmsuCG.6.1	A5.4	ORP.5.A2	COM-03
NIS2UmsuCG.6.2	A6.3	ORP.3.A1	HR-03
NIS2UmsuCG.7	A5.5, A5.31	ORP.5.A1, ORP.5.A2	COS-01

Kennung	ISO 27001	IT-Grundschutz-Kompendium	C5-Katalog
BSIG.1.1	A5.1, A5.2, A5.3, A5.6, A5.9, A5.10, A5.11, A5.12, A5.13, A.5.36, A6.2, A6.3, A6.4, A6.5, A7.1, A7.2, A7.3, A7.4, A7.10, A,8.6, A8.9, A8.10, A8.14, A8.20, A8.24, A8.26, A8.34	OPS.1.1.1.A9, DER.1.A5, DER.1.A6, SYS.1.1.A27, DER.2.1.A9, DER.2.3, ISMS.1, ORP.4.A4, ORP.4.A6, ORP.4.A7	OIS, AM, BCM, IDM, CRY, COS, HR, PS, SIM, COM
BSIG.1.2	A8.16	OPS.1.1.1.A9, DER.1.A5, DER.1.A6, DER.1.A15, SYS.1.1.A27	OPS-13
BSIG.1.3	A5.5, A5.31	ORP.5.A1, ORP.5.A2	COM-01

Tabelle B.1: Katalog: Anforderungen und Maßnahmen