Vergleich der Umsetzung von Art. 21 Abs. 2 der NIS2-Richtlinie Stand: 5.12.2025
im NIS-2-Umsetzungsgesetz (§ 30 Abs 2 BSIG, §165 Abs. 2a TKG und § 5c Abs. 3 EnWG) sowie
die Zuordnung der technischen und methodischen Anforderungen gemäß Art. 2 der Durchführungsverordnung (EU) 2024/2590 der Kommission

Art. 21 Abs. 2 NIS2-Richtlinie[1]	§ 30 Abs. 2 BSI-Gesetz[2]	§ 165 Abs. 2a TKG[3]	§ 5c Abs. 3 EnWG[4]	Durchführungsverordnung (EU) 2024/2690 der Kommission[5]
Die in Absatz 1 genannten Maßnahmen müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und zumindest Folgendes umfassen:	Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen~~, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen~~. Die Maßnahmen müssen zumindest Folgendes umfassen:	Maßnahmen nach Absatz 2 von Betreibern öffentlicher Telekommunikationsnetze und Anbietern öffentlich zugänglicher Telekommunikationsdienste, die besonders wichtige Einrichtungen im Sinne von § 28 Absatz 1 Satz 1 Nummer 3 des BSI-Gesetzes oder wichtige Einrichtungen im Sinne von § 28 Absatz 2 Satz 1 Nummer 2 des BSI-Gesetzes sind, müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und zumindest Folgendes umfassen:	Der IT-Sicherheitskatalog hat mindestens Vorgaben zu enthalten für:	*(Die Vorgaben gelten nur für DNS-Diensteanbieter, TLD-Namenregister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter verwalteter Dienste, Anbieter verwalteter Sicherheitsdienste, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter)*
Konzept für die Sicherheit von Netz- und Informationssystemen (Buchstabe a)				
a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;	1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,	1. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme,	1. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationstechnik,	*1.1. Konzept für die Sicherheit von Netz- und Informationssystemen* *1.2. Rollen, Verantwortlichkeiten und Weisungsbefugnisse*
Konzept für das Risikomanagement (Buchstabe a)				
				2.1. Risikomanagementrahmen *2.2. Überwachung der Einhaltung* *2.3. Unabhängige Überprüfung der Netz- und Informationssicherheit*

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555
[2] Art. 1 des Gesetzes vom 2.12.2025 (BGBl. 2025 I Nr. 301) (https://www.recht.bund.de/eli/bund/bgbl-1/2025/301)
[3] Art. 25 des Gesetzes vom 2.12.2025 (BGBl. 2025 I Nr. 301)
[4] Art. 17 des Gesetzes vom 2.12.2025 (BGBl. 2025 I Nr. 301)
[5] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202402690

Bewältigung von Sicherheitsvorfällen (Buchstabe b)				
b) Bewältigung von Sicherheitsvorfällen;	2. Bewältigung von Sicherheitsvorfällen,	2. Bewältigung von Sicherheitsvorfällen,	2. die Bewältigung von Sicherheitsvorfällen,	*3.1. Konzept für die Bewältigung von Sicherheitsvorfällen* *3.2. Überwachung und Protokollierung* *3.3. Meldung von Ereignissen* *3.4. Bewertung und Klassifizierung von Ereignissen* *3.5. Reaktion auf Sicherheitsvorfälle* *3.6. Überprüfungen nach Sicherheitsvorfällen*
Betriebskontinuitäts- und Krisenmanagement (Buchstabe c)				
c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;	3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,	3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,	3. die Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und das Krisenmanagement,	*4.1. Notfallplan für die Aufrechterhaltung und Wiederherstellung des Betriebs* *4.2. Backup-Sicherungs- und Redundanzmanagement* *4.3. Krisenmanagement*
Sicherheit der Lieferkette (Buchstabe d)				
d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;	4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen ~~zwischen den einzelnen Einrichtungen und ihren~~ zu unmittelbaren Anbietern oder Diensteanbietern,	4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,	4. die Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,	*5.1. Konzept für die Sicherheit der Lieferkette* *5.2. Verzeichnis der Anbieter und Diensteanbieter*
Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen (Buchstabe e)				
e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;	5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,	5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen,	5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen,	*6.1. Sicherheitsmaßnahmen beim Erwerb von IKT-Diensten oder IKT-Produkten* *6.2. Sicherer Entwicklungszyklus* *6.3. Konfigurationsmanagement* *6.4. Änderungsmanagement, Reparatur und Wartung* *6.5. Sicherheitsprüfung* *6.6. Sicherheitspatch-Management* *6.7. Netzsicherheit* *6.8. Netzsegmentierung* *6.9. Schutz gegen Schadsoftware und nicht genehmigte Software*

				6.10. Behandlung und Offenlegung von Schwachstellen
Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit (Buchstabe f)				
f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;	6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,	6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Maßnahmen nach Absatz 2 im Bereich der Sicherheit von Netzen und Diensten,	6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit der Informationstechnik,	*7.1. [Konzept und Verfahren für wirksame Umsetzung Risikomanagementmaßnahmen im Bereich der Cybersicherheit]* *7.2. die entsprechenden Verfahren tragen den Ergebnissen der Risikobewertung gemäß Nummer 2.1 und früheren erheblichen Sicherheitsvorfällen Rechnung.* *7.3.[Überprüfung des Konzepts und die Verfahren in geplanten Zeitabständen sowie bei erheblichen Sicherheitsvorfällen, wesentlichen Änderungen der Betriebsabläufe oder der Risiken]*
Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit (Buchstabe g)				
g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;	7. grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik,	7. Grundlegende Verfahren und Schulungen im Bereich der Sicherheit von Netzen und Diensten,	7. grundlegende Verfahren im Bereich der Cyberhygiene und für Schulungen im Bereich der Sicherheit der Informationstechnik	*8.1. Sensibilisierungsmaßnahmen und grundlegende Verfahren im Bereich der Cyberhygiene* *8.2. Sicherheitsschulungen*
Kryptografie (Buchstabe h)				
h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;	8. Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren,	8. Konzepte und Verfahren für den Einsatz von Kryptografie und ~~gegebenenfalls~~ Verschlüsselung,	8. Konzepte und Verfahren für den Einsatz von Kryptografie und ~~gegebenenfalls~~ Verschlüsselung,	*9.1. [Konzepte und Verfahren für eine angemessene und wirksame Nutzung von Kryptografie]* *9.2. [Details der Inhalte der Konzepte und Verfahren]*
Sicherheit des Personals (Buchstabe i)				
i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;	9. Erstellung von Konzepten für die Sicherheit des Personals, die Zugriffskontrolle und für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen,	9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen,	9. die Sicherheit des Personals, Konzepte für die Zugriffskontrolle und das Management von Anlagen,	*10.1. Sicherheit des Personals* *10.2. Zuverlässigkeitsüberprüfung* *10.3. Verfahren zur Beendigung oder Änderung des Beschäftigungsverhältnisses* *10.4. Disziplinarverfahren*
Anlagen- und Wertemanagement (Buchstabe i)				
				12.1. Anlagen- und Werteklassifizierung *12.2. Behandlung von Anlagen und Werten* *12.3. Konzept für Wechseldatenträger*

				12.4. Anlagen- und Werteinventar *12.5. Abgabe, Rückgabe oder Löschung von Anlagen und Werten bei Beendigung des Beschäftigungsverhältnisses*
Zugriffskontrolle (Buchstaben i und j)				
j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.	10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.	10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.	10. die Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung,	*11.1. Konzept für die Zugriffskontrolle* *11.2. Management von Zugangs- und Zugriffsrechten* *11.3. Privilegierte Konten und Systemverwaltungskonten* *11.4. Systemverwaltungssysteme* *11.5. Identifizierung* *11.6. Authentifizierung* *11.7. Multifaktor-Authentifizierung*
Sicherheit des Umfelds und physische Sicherheit (Buchstaben c, e und i)				
				13.1. Unterstützende Versorgungsleistungen *13.2. Schutz vor physischen Bedrohungen und Bedrohungen des Umfelds* *13.3. Perimeter und physische Zutrittskontrolle*
Keine vergleichbare Vorschrift	*§ 31 Abs. 2 für Betreiber kritischer Anlagen enthält eine vergleichbare Vorschrift („Betreiber kritischer Anlagen sind verpflichtet, für die informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Anlagen maßgeblich sind, Systeme zur Angriffserkennung einzusetzen. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie*	*§ 165 Abs. 3 enthält bereits vor der Novelle eine vergleichbare Vorschrift („Als eine angemessene Maßnahme im Sinne des Absatzes 2 können Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste Systeme zur Angriffserkennung im Sinne des § 2 Absatz 9b des BSI-Gesetzes einsetzen. Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste mit erhöhtem Gefährdungspotenzial haben entsprechende Systeme zur Angriffserkennung einzusetzen. Die eingesetzten Systeme*	11. den Einsatz von Systemen zur Angriffserkennung nach § 2 Nummer 41 des BSI-Gesetzes,	*./.*

	für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. Dabei soll der Stand der Technik eingehalten werden. Der hierfür erforderliche Aufwand soll nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage stehen.“)	*zur Angriffserkennung müssen in der Lage sein, durch kontinuierliche und automatische Erfassung und Auswertung Gefahren oder Bedrohungen zu erkennen. Sie sollen zudem in der Lage sein, erkannte Gefahren oder Bedrohungen abzuwenden und für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen. Weitere Einzelheiten kann die Bundesnetzagentur im Katalog von Sicherheitsanforderungen nach § 167 festlegen.“)*		
Kann-Vorgabe aus Art. 24 Abs.1 („Die Mitgliedstaaten können wesentliche und wichtige Einrichtungen dazu verpflichten, spezielle IKT-Produkte, -Dienste und -Prozesse zu verwenden, die von der wesentlichen oder wichtigen Einrichtung entwickelt oder von Dritten beschafft werden und die im Rahmen europäischer Schemata für die Cybersicherheitszertifizierung, die gemäß Artikel 49 der Verordnung (EU) 2019/881 angenommen wurden, zertifiziert sind, um die Erfüllung bestimmter in Artikel 21 genannter Anforderungen nachzuweisen. Darüber hinaus fördern die Mitgliedstaaten, dass wesentliche und wichtige Einrichtungen qualifizierte Vertrauensdienste nutzen.“)	*§ 30 Abs. 6 führt eine vergleichbare Regelung über eine Verordnungsermächtigung ein („Besonders wichtige Einrichtungen und wichtige Einrichtung dürfen durch Rechtsverordnung nach § 56 Absatz 3 bestimmte IKT-Produkte, IKT-Dienste und IKT-Prozesse nur verwenden, wenn diese über eine Cybersicherheitszertifizierung gemäß europäischer Schemata nach Artikel 49 der Verordnung (EU) 2019/881 verfügen.“)*	*§ 165 Abs. 4 enthält bereits vor der Novelle eine Vorschrift, die eine Zertifizierung (aber keine Cybersicherheitszertifizierung gemäß Art. 49 der Verordnung (EU) 2019/881) verlangt:* *(Kritische Komponenten im Sinne von § 2 Absatz 13 des BSI-Gesetzes dürfen von einem Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial nur eingesetzt werden, wenn sie vor dem erstmaligen Einsatz von einer anerkannten Zertifizierungsstelle überprüft und zertifiziert wurden.)*	12. den Einsatz eines Elements oder einer Gruppe von Elementen eines Netz- oder Informationssystems (IKT-Produkt), eines Dienstes, der vollständig oder überwiegend aus der Übertragung, Speicherung, Abfrage oder Verarbeitung von Informationen mittels Netz- und Informationssystemen besteht (IKT-Dienst), und jeglicher Tätigkeiten, mit denen ein IKT-Produkt oder ein IKT-Dienst konzipiert, entwickelt, bereitgestellt oder gepflegt werden soll (IKT-Prozess), mit Cybersicherheitszertifizierung gemäß europäischer Schemata nach Artikel 49 der Verordnung (EU) 2019/881.	*./.*