

# **Nationale Risikoanalyse gem. RKEG 2026**

Wien, 2026

## **Impressum**

Medieninhaber, Verleger und Herausgeber:

Bundesministerium für Inneres, Herrngasse 7, 1010 Wien

Wien, 2026. Stand: 19. Jänner 2026

### **Copyright und Haftung:**

Auszugsweiser Abdruck ist nur mit Quellenangabe gestattet, alle sonstigen Rechte sind ohne schriftliche Zustimmung des Medieninhabers unzulässig.

Es wird darauf verwiesen, dass alle Angaben in dieser Publikation trotz sorgfältiger Bearbeitung ohne Gewähr erfolgen und eine Haftung des Bundesministeriums und der Autorin / des Autors ausgeschlossen ist. Rechtausführungen stellen die unverbindliche Meinung der Autorin / des Autors dar und können der Rechtsprechung der unabhängigen Gerichte keinesfalls vorgreifen.

## Inhalt

<b>Executive Summary</b> .....	<b>5</b>
<b>1 Einleitung</b> .....	<b>6</b>
<b>2 Grundlagen und Rahmenbedingungen</b> .....	<b>9</b>
2.1 ISO 31000 – Grundsätze, Rahmenwerk und Prozess.....	9
2.2 ÖNORM Reihe D 4900 .....	10
2.3 Gesetzlicher Rahmen – RKEG und RKE-Richtlinie.....	12
2.4 Europäische Rechtsgrundlagen sektoraler Risikoanalysen .....	15
2.5 Begriffe und Definitionen .....	22
<b>3 Kontext Österreich</b> .....	<b>24</b>
Anforderungen gemäß ÖNORM D 4901 Normpunkt 4.....	24
3.1 Politischer, wirtschaftlicher und gesellschaftlicher Kontext .....	24
3.1.1 Politischer Kontext .....	24
3.1.2 Wirtschaftlicher Kontext .....	26
3.1.3 Gesellschaftlicher Kontext.....	26
3.2 Geografische und ökologische Rahmenbedingungen .....	27
3.3 Stakeholderanalyse.....	30
3.4 Historische Risikoanalyse.....	31
3.5 Nationaler Gefahrenkatalog .....	33
<b>4 Risikomanagementsystem – Organisation &amp; Struktur</b> .....	<b>36</b>
Anforderungen gemäß ÖNORM D 4901 Normpunkte 5-7.....	36
4.1 Führungsaufgabe und Governance .....	36
4.2 Rollen und Verantwortlichkeiten.....	37
4.3 Integration in nationale Strategien und Systeme.....	39
<b>5 Risikomanagementprozess</b> .....	<b>41</b>
Anforderungen gemäß ÖNORM D 4901 Normpunkt 8.....	41
5.1 Prozessübersicht.....	41
5.2 Kommunikation und Konsultation.....	43
5.3 Rahmenbedingung und Risikokriterien .....	44
5.4 Risikoidentifikation .....	45
5.5 Risikoanalyse.....	46
5.6 Risikobewertung .....	48
5.7 Risikobehandlung.....	49
5.8 Überwachung und Review .....	49

<b>6 Risikobewertung &amp; Ergebnisse.....</b>	<b>51</b>
Anforderungen gemäß ÖNORM D 4901 Normpunkt 9.....	51
6.1 Risiken nach Sektoren und Teilsektoren.....	52
6.2 Sektorübergreifenden Auswirkungen.....	67
6.3 Risiken mit grenzüberschreitenden Auswirkungen.....	69
6.4 Klimawandelbedingte Risiken.....	70
6.5 Low Probability/High Impact Risks .....	72
6.6 Emerging Risks .....	72
6.7 Darstellung der Risikomatrix.....	73
<b>7 Dokumentation und Kommunikation.....</b>	<b>76</b>
Anforderungen gemäß ÖNORM D 4901 Normpunkt 10.....	76
<b>8 Schlussfolgerung und Ausblick.....</b>	<b>78</b>
<b>Literaturverzeichnis .....</b>	<b>79</b>
<b>Abkürzungen.....</b>	<b>87</b>
<b>Anhang 1: Liste der Sektoren inklusive wesentlicher Dienste gemäß Delegierter Verordnung (EU) 2023/2450.....</b>	<b>88</b>
<b>Anhang 2: Skalierung von Eintrittswahrscheinlichkeit und Auswirkung .....</b>	<b>94</b>
<b>Anhang 3: Risikomatrix .....</b>	<b>97</b>
<b>Anhang 4: nationaler Gefahrenkatalog .....</b>	<b>98</b>
Naturgefahren .....	99
Anthropogene Gefahren .....	105
Intentionale Gefahren .....	119
Technische Gefahren.....	131

# Executive Summary

Die nationale Risikoanalyse für kritische Einrichtungen 2026 wurde im Rahmen des Resilienz kritischer Einrichtungen-Gesetzes (RKEG) erstellt und ist gleichzeitig die Ergänzung des Masterplanes des Österreichischen Programmes zum Schutz kritischer Infrastrukturen (APCIP) aus dem Jahr 2014 und der daraus resultierenden staatlichen Risikoanalyse für kritische Einrichtungen 2022. Sie basiert auf der internationalen Norm ISO 31000 und der nationalen ÖNORM Reihe D 4900 und erfüllt damit sowohl gesetzliche als auch normative Anforderungen.

Ziel dieser Risikoanalyse ist es, eine gesamtstaatliche Makro-Sicht zu liefern, die als strategische Grundlage für Politik, Verwaltung und kritische Einrichtungen dient. Während der Staat die Gefahrenlage und sektorübergreifende Risiken darstellt, sind die kritischen Einrichtungen verpflichtet, auf dieser Basis eigene Risikoanalysen durchzuführen und Resilienzmaßnahmen umzusetzen.

Diese Risikoanalyse identifiziert Gefahren im Rahmen des All-Gefahren-Ansatzes (All-Hazards-Approach) und berücksichtigt dabei natürliche, technische, gesellschaftliche, cyber-bezogene und geopolitische Entwicklungen. Besondere Schwerpunkte liegen auf Risiken mit sektorübergreifenden und grenzüberschreitenden Auswirkungen, klimawandelbedingten Gefahren sowie seltenen Ereignissen mit hohem Schadenspotenzial („Low Probability/High Impact“-Risiken). Emerging Risks werden ebenso systematisch in den Analyseprozess integriert.

Die Ergebnisse werden nach Sektoren und Teilsektoren gegliedert und liefern eine Priorisierung der relevantesten Risiken für kritische Einrichtungen in Österreich. Damit schafft diese Risikoanalyse die Grundlage für eine kohärente nationale Strategie für die Resilienz kritischer Einrichtungen und unterstützt gleichzeitig kritische Einrichtungen bei der Erfüllung ihrer Pflichten.

Die Risikoanalyse folgt einem transparenten, normkonformen Aufbau auf wissenschaftlicher Basis und greift auf nationale und internationale Risikoanalysen und Sicherheitsberichte (bspw. Deutschland, Schweiz, EU) zurück. Sie ermöglicht somit eine fundierte Bewertung der nationalen Gefährdungslage und stellt ein transparentes, nachhaltiges und prüffähiges Dokument dar.

# 1 Einleitung

Die vorliegende nationale Risikoanalyse für die Republik Österreich verfolgt das Ziel, eine nationale Risikoübersicht für kritische Einrichtungen zu schaffen. Sie bildet einen staatlichen Orientierungsrahmen, auf dessen Basis jede kritische Einrichtung eine eigene Risikoanalyse<sup>1</sup> durchführen muss.

Während diese nationale Risikoanalyse die gesamtstaatliche Perspektive („Makro-Sicht“) gemäß § 10 RKEG abbildet, sind die kritischen Einrichtungen verpflichtet, diese Ergebnisse auf ihre spezifischen Systeme gemäß § 14 RKEG zu übertragen („Mikro-Sicht“).

Diese Risikoanalyse erfüllt den gesetzlichen Auftrag des Resilienz kritischer Einrichtungen-Gesetzes (RKEG)<sup>2</sup>, dass die RKE-Richtlinie (EU) 2022/2557<sup>3</sup> in nationales Recht umsetzt. Gemäß § 10 RKEG ist der Bundesminister für Inneres verpflichtet, eine nationale Risikoanalyse zu erstellen, die alle relevanten Gefahren systematisch erfasst. Diese Analyse ist zugleich mögliche Grundlage für die Erstellung einer Risikoanalyse durch kritische Einrichtungen gemäß § 14 RKEG.

Diese Risikoanalyse verfolgt drei Hauptziele:

1. Bereitstellung eines nationalen Gefahrenkatalogs, der kritischen Einrichtungen ermöglicht, Gefahren in konkrete Gefährdungen zu übersetzen und Risiken abzuleiten.<sup>4</sup>
2. Stringenz nach ISO 31000:2018<sup>5</sup> und der ÖNORM Reihe D 4900:2021<sup>6</sup>, mit expliziten Verweisen auf Normpunkte und Normen des RKEG.
3. Sicherung der Nachvollziehbarkeit durch klaren Normbezug ermöglicht eine kontinuierliche, nachhaltige Weiterentwicklung der nationalen Risikoanalyse.

---

<sup>1</sup> § 14 RKEG

<sup>2</sup> Bundesgesetz zur Sicherstellung eines hohen Resilienznieaus von kritischen Einrichtungen (Resilienz kritischer Einrichtungen-Gesetz – RKEG), BGBl. I Nr. 60/2025.

<sup>3</sup> Richtlinie (EU) 2022/2557 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates, ABl. Nr. L 333 vom 27.12.2022 S. 164.

<sup>4</sup> Aven, T. (2015).

<sup>5</sup> International Organization for Standardization (2018).

<sup>6</sup> Austrian Standards International (2021).

Adressaten sind die österreichischen Bundesministerien, die österreichischen Landes- und Sicherheitsbehörden, die kritischen Einrichtungen sowie gesetzliche Interessenvertretungen.

Diese Risikoanalyse stützt sich methodisch auf drei zentrale Säulen:

- ISO 31000:2018 als internationalen Rahmen für Risikomanagement,
- ÖNORM Reihe D 4900 als nationale Präzisierung
- RKEG zur Umsetzung der RKE-Richtlinie

Ihre wissenschaftliche Fundierung erfolgt durch internationale Vergleichsstudien und einschlägige Fachliteratur. Zusätzlich haben die nationalen Risikoanalysen in Deutschland<sup>7</sup> und in der Schweiz<sup>8</sup> eine methodische Orientierung geboten. Ergänzend fließen Grundlagenwerke zum Risikobegriff, zu Resilienz und Managementsystemen ein.<sup>9</sup>

Diese Risikoanalyse ist eine staatliche Risikoanalyse und ersetzt nicht die Risikoanalysen der kritischen Einrichtungen. Sie beschreibt Gefahren nach dem All-Gefahren-Ansatz des RKEG, demnach sind beispielsweise Naturereignisse, technische Gefahren, gesellschaftliche Gefahren, Cyberattacken, intentionale Gefahren, anthropogene Gefahren und geopolitische Entwicklungen inbegriffen.

Darüber hinaus berücksichtigt diese Risikoanalyse neu auftretende Risiken (Emerging Risks), also Gefahren, die in Folge technologischer, gesellschaftlicher oder ökologischer Veränderungen entstehen und bisher nur unzureichend erfasst wurden.<sup>10</sup> Da in der RKE Richtlinie und im RKEG der Umgang mit klimawandelbedingte Risiken, durch welche die Zunahme von Extremwetterereignissen und langfristigen Umweltveränderungen stetig wächst<sup>11</sup>, besonders hervorgehoben ist, wurde ein besonderer Fokus auf die Bedeutung und dem Umgang dieser Risiken gelegt.

---

<sup>7</sup> BBK (2022).

<sup>8</sup> BABS (2019).

<sup>9</sup> Aven, T. (2015); Linkov, I. / Trump, B. D. (2019); Renn, O. (2017); Hubbard, D. (2020).

<sup>10</sup> OECD (2018).

<sup>11</sup> IPCC (2021).

Ergänzend werden Ereignisse mit geringer Eintrittswahrscheinlichkeit, aber potenziell sehr hohen Auswirkungen, sogenannte „Low-Probability/High-Impact-Risiken“<sup>12</sup> in die Analyse einbezogen, da sie für die nationale Resilienzplanung von entscheidender Relevanz sind.

Die in dieser Risikoanalyse dargestellten Bewertungen und sektoralen Ergebnisse sind als qualifizierte Zwischenstände zu verstehen. Zum Zeitpunkt der Erstellung lagen für mehrere Sektoren noch keine vollständig validierten Datensätze vor, da Workshops mit potenziell kritischen Einrichtungen teilweise noch im Laufen sind und die endgültige Identifikation der kritischen Einrichtungen gemäß RKEG noch nicht abgeschlossen ist. Erst nach Abschluss dieser Erhebungs- und Konsultationsprozesse kann eine vollständige, abschließende und final validierte Risikobewertung vorgelegt werden. Die vorliegenden Ergebnisse basieren daher auf der besten aktuell verfügbaren Datenlage und werden im Rahmen der laufenden Aktualisierungsschritte in den folgenden 4 Jahren weiter präzisiert.

Damit ist diese Risikoanalyse ein wissenschaftlich fundiertes, normkonformes und rechtlich verankertes Instrument, das für Politik, Verwaltung, kritische Einrichtungen und Gesellschaft gleichermaßen von zentraler Bedeutung ist.

---

<sup>12</sup> Renn, O. (2017).

# 2 Grundlagen und Rahmenbedingungen

Kapitel 2 legt die methodischen, normativen und rechtlichen Grundlagen dieser Risikoanalyse fest. Es erläutert die internationalen, nationalen und rechtlichen Bezugssysteme, auf denen die Risikoanalyse aufbaut. In Unterkapitel 2.1 wird die ISO 31000:2018 vorgestellt, die als internationaler Referenzrahmen für Risikomanagementprinzipien, -prozesse und -governance dient. Unterkapitel 2.2 beschreibt die ÖNORM D 4900 – D 4903:2021, welche die ISO-Vorgaben für Österreich präzisiert und um nationale Anforderungen ergänzt. In Unterkapitel 2.3 wird der rechtliche Rahmen dargestellt, insbesondere das RKEG als Umsetzung der RKE-Richtlinie, dass die rechtliche Verpflichtung zur Durchführung nationaler und betrieblicher Risikoanalysen regelt. Schließlich werden in Unterkapitel 2.4 die zentralen Begriffe und Definitionen harmonisiert, um sicherzustellen, dass alle Akteure mit einem einheitlichen Verständnis operieren. Damit schafft Kapitel 2 die notwendige Kohärenz zwischen Standards, Normen und gesetzlichen Anforderungen und bildet den normativen Rahmen, auf dem alle weiteren Kapitel dieser Risikoanalyse aufbauen.

## 2.1 ISO 31000 – Grundsätze, Rahmenwerk und Prozess

Die ISO 31000 bildet den zentralen internationalen Referenzstandard für das Risikomanagement. Sie definiert Grundsätze, ein organisatorisches Rahmenwerk sowie den Risikomanagementprozess, die in sämtlichen Organisationen, von staatlichen Behörden bis hin zu privatwirtschaftlichen Akteuren, anwendbar sind. Dieser Risikoanalyse orientiert sich in Aufbau und Methodik unmittelbar an dieser Norm, um eine internationale Vergleichbarkeit und Auditierbarkeit sicherzustellen.

Die ISO 31000 versteht Risikomanagement als einen systematischen, transparenten und wiederholbaren Prozess, der in alle Entscheidungs- und Steuerungsprozesse integriert werden muss. Sie betont, dass Risiken nicht ausschließlich negative Abweichungen darstellen, sondern auch Chancen umfassen können, ein Aspekt, der für eine betriebliche Risikoanalyse

von kritischen Einrichtungen insofern bedeutsam ist, als er auch Potenziale für Resilienzsteigerung aufzeigt.<sup>13</sup>

Der gegenständliche Standard ist in drei zentrale Bereiche gegliedert:

- Grundsätze (Principles): Diese bilden die normative Basis und verlangen, dass Risikomanagement wertschöpfend, strukturiert, integriert, dynamisch und transparent durchgeführt wird. Besonders relevant für staatliche Risikoanalysen sind die Prinzipien der Integration, Inklusion und kontinuierlichen Verbesserung, die sicherstellen, dass das Risikomanagement nicht isoliert, sondern als Teil einer übergeordneten Governance-Struktur verstanden wird.
- Rahmenwerk (Framework): Dieses beschreibt die organisatorischen Voraussetzungen, die zur Implementierung eines wirksamen Risikomanagementsystems erforderlich sind. Dazu zählen Rollen und Verantwortlichkeiten, Ressourcenmanagement, Kommunikation, Berichterstattung und die Integration in bestehende Managementsysteme.
- Prozess (Process): Der eigentliche Risikomanagementprozess umfasst die Phasen Kommunikation und Konsultation, Festlegung des Kontextes, Risikoidentifikation, Risikobewertung, Risikobehandlung sowie Überwachung und Überprüfung. Diese Struktur bildet das methodische Rückgrat dieser Risikoanalyse und wird in Kapitel 5 detailliert auf staatliche Anforderungen übertragen.

Durch ihre Anwendung gewährleistet die ISO 31000, dass diese Risikoanalyse ein einheitliches und international nachvollziehbares Risikomanagementverständnis verfolgt. Ihre Prinzipien der Transparenz, Nachvollziehbarkeit und ständigen Verbesserung schaffen die methodische Grundlage für eine nachhaltige nationale Risikoanalyse.<sup>14</sup>

## 2.2 ÖNORM Reihe D 4900

Die ÖNORM-Reihe D 4900 konkretisiert die ISO 31000 für den österreichischen Kontext und übersetzt deren Grundsätze in ein praktisch anwendbares, landesspezifisches Rahmenwerk. Während die ISO 31000 international allgemein gehalten ist, schafft die ÖNORM Reihe D

---

<sup>13</sup> Aven, T. (2015).

<sup>14</sup> Renn, O. (2017).

4900 verbindliche Terminologien, klare Prozessdefinitionen und integrationsfähige Managementstrukturen, die auf nationale Bedürfnisse abgestimmt sind.

Die ÖNORM Reihe D 4900 gliedert sich in mehrere komplementäre Teile, die zusammen das Fundament für ein kohärentes Risikomanagementsystem bilden:

ÖNORM D 4900 legt die zentralen Begriffe fest und harmonisiert diese mit den internationalen Standards, um ein einheitliches Verständnis zwischen allen Benutzerinnen und Benutzern sicherzustellen.

ÖNORM D 4901 beschreibt die Anforderungen an Aufbau, Implementierung und kontinuierliche Verbesserung von Risikomanagementsystemen in Organisationen. Sie stellt sicher, dass Risikoanalysen planmäßig durchgeführt und in Entscheidungsprozesse integriert werden.

ÖNORM D 4902-Teil 1 bis 3 vertiefen den methodischen Teil. Sie spezifizieren Verfahren zur Risikoidentifikation, -bewertung und -behandlung sowie qualitative und quantitative Bewertungsmodelle, einschließlich Unsicherheitsanalysen.

ÖNORM D 4903 definiert Rollen, Verantwortlichkeiten und Qualifikationsanforderungen für Personen, die mit Risikomanagementaufgaben betraut sind.

Im Gegensatz zur ISO 31000, die überwiegend prozessual-konzeptionell ist, besitzt die ÖNORM Reihe D 4900 eine operative und implementierungsorientierte Ausrichtung. Dadurch eignet sie sich besonders für staatliche Anwendungen, wie sie im Rahmen von nationalen Risikoanalysen erforderlich sind. Sie stellen sicher, dass diese Risikoanalyse sowohl strategisch normenkonform als auch praktisch umsetzbar bleibt.<sup>15</sup>

Ein weiterer wesentlicher Beitrag der ÖNORM Reihe D 4900 liegt in der Integration von Risikomanagement in bestehende Managementsysteme. Dadurch wird das Risikomanagement nicht als isolierte Funktion betrachtet, sondern als Bestandteil der Organisationsführung. Dieser Ansatz gilt in der internationalen Forschung als entscheidend für die Effektivität staatlicher und unternehmensinterner Risikostrukturen.<sup>16</sup>

---

<sup>15</sup> Bartz, H.-J. (2022).

<sup>16</sup> Frigo, M. L. / Anderson, R. J. (2011).

In dieser Risikoanalyse wird die ÖNORM Reihe D 4900 genutzt, um den Übergang von strategischen Prinzipien zu operativen Prozessen zu gestalten. Sie dient als Brücke zwischen der ISO 31000 als internationalem Bezugsrahmen und dem RKEG als rechtlicher Grundlage. Dadurch entsteht ein kohärentes System, das rechtliche Verbindlichkeit, methodische Strenge und organisatorische Praktikabilität vereint.

## 2.3 Gesetzlicher Rahmen – RKEG und RKE-Richtlinie

Die Rechtsgrundlagen, auf der diese Risikoanalyse basiert, besteht aus zwei komplementären Ebenen, der europäischen RKE-Richtlinie und ihrer nationalen Umsetzung durch das RKEG. Zusammen bilden sie das gesetzliche Fundament, das die Pflicht zur Durchführung dieser Risikoanalyse und der betrieblichen Risikoanalysen der kritischen Einrichtungen festlegt.

Im europäischen Kontext ist Artikel 5 der RKE-Richtlinie zentral. Er verpflichtet jeden Mitgliedstaat, regelmäßig eine nationale Risikoanalyse durchzuführen, um Gefahren und Risiken zu identifizieren, die kritische Einrichtungen oder wesentliche Dienste beeinträchtigen können. Diese Risikoanalyse muss sich auf den All-Gefahren-Ansatz stützen und sowohl intentionale als auch nicht-intentionale Bedrohungen, hybride, technologische und klimabedingte Risiken berücksichtigen.

Die Verpflichtung zur Durchführung einer Risikoanalyse ergibt sich aus § 10 RKEG. Der Bundesminister für Inneres ist verpflichtet, auf Grundlage der in § 3 Z 6 RKEG definierten wesentlichen Dienste<sup>17</sup> eine nationale Risikoanalyse zu erstellen. Diese Risikoanalyse muss

---

<sup>17</sup> „wesentlicher Dienst“ iSd § 3 Z 6 RKEG: ein Dienst, der in der Delegierten Verordnung (EU) 2023/2450 zur Ergänzung der Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates durch eine Liste wesentlicher Dienste, ABl. Nr. L 2023/2450 vom 30.10.2023, festgelegt wurde; darüber hinaus allfällige weitere aufgrund einer Verordnung des Bundesministers für Inneres festgelegte Dienste, die für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, wichtiger wirtschaftlicher Tätigkeiten, der öffentlichen Gesundheit und Sicherheit oder die Erhaltung der Umwelt von erheblicher Bedeutung sind und von einer Einrichtung der im Anhang der RKE-RL angeführten Kategorien in den gelisteten Sektoren und Teilsektoren erbracht werden.

erstmalig spätestens bis zum 17. Jänner 2026 vorliegen und danach anlassbezogen, spätestens aber alle vier Jahre aktualisiert werden. Diese Risikoanalyse ist nach den im Anhang der RKE-Richtlinie, gelisteten Sektoren und Teilsektoren aufzuschlüsseln (siehe Anhang 1).

Damit legt das RKEG eine strukturierte sektorale Gliederung der nationalen Risikoanalyse fest, die europaweit harmonisiert ist.

Bevor die Risikoanalyse abgeschlossen wird, sind den

- im jeweiligen Wirkungsbereich betroffenen Bundesministerien,
- den betroffenen Ländern und
- den in Betracht kommenden Interessenvertretungen

Gelegenheit zur Äußerung zu geben.

Damit wird der Art. 5 der RKE-Richtlinie direkt umgesetzt, der den Bundesminister für Inneres verpflichtet, bis 17. Jänner 2026 erstmalig eine nationale Risikoanalyse zu erstellen.

Der Bundesminister für Inneres muss gesetzlich bei der Erstellung der Risikoanalyse vier zentrale Informationsquellen und Analyseebenen berücksichtigen. Es sind die Ergebnisse der nach Art. 6 Abs. 1 des Beschlusses Nr. 1313/2013/EU durchgeführten allgemeinen Risikoanalyse im Rahmen des EU-Katastrophenschutzverfahrens zu berücksichtigen. Diese europäische Risikoanalyse dient der Identifikation und Bewertung grenzüberschreitender Risiken und schafft damit die Grundlage für die Kohärenz zwischen dieser Risikoanalyse und der europäischen Katastrophenvorsorgeplanung. Diese Risikoanalyse baut auf bestehende europäische Gefahreneinschätzungen auf und muss mit diesen inhaltlich kompatibel sein.

Es sind Risikoanalysen zu berücksichtigen, die im Einklang mit einschlägigen sektorspezifischen EU-Rechtsakten durchgeführt werden. Das RKEG nennt ausdrücklich:

- Verordnung (EU) 2019/941 über die Risikovorsorge im Elektrizitätssektor,
- Verordnung (EU) 2017/1938 über Maßnahmen zur sicheren Gasversorgung,
- Richtlinie 2012/18/EU (Seveso III) zur Beherrschung von Gefahren schwerer Unfälle mit gefährlichen Stoffen,
- Richtlinie 2007/60/EG über die Bewertung und das Management von Hochwasserrisiken.

Aufgrund dessen muss diese Risikoanalyse keine isolierte nationale Betrachtung sein, sondern muss bestehende sektorspezifische Risikoanalysen der EU vollständig integrieren. Dadurch werden Doppelanalysen vermieden und Synergien zwischen europäischer und nationaler Risikopolitik geschaffen.

Berücksichtigt werden müssen die Risiken, die sich aus der gegenseitigen Abhängigkeit der Sektoren untereinander ergeben, sowie die Abhängigkeiten von kritischen Einrichtungen in anderen Mitgliedstaaten oder Drittstaaten. Außerdem sind die Auswirkungen eines Sicherheitsvorfalls<sup>18</sup> in einem Sektor auf andere Sektoren zu erfassen (Kaskadeneffekte)<sup>19</sup>. Eine systemische Sichtweise wird eindeutig gefordert. Diese Risikoanalyse muss sektorübergreifende und transnationale Wechselwirkungen abbilden. Das umfasst sowohl physische als auch digitale Abhängigkeiten, bspw. zwischen Energiesektor, Bankensektor und Gesundheitssektor. Dieser Ansatz deckt sich mit den Prinzipien des „Systemic Risk Management“ von *Linkov/B.D. Trump* aus dem Jahr 2019.<sup>20</sup>

Alle gemäß § 17 RKEG zu meldenden Sicherheitsvorfälle sind künftig in die Risikoanalyse einzubeziehen. Das bedeutet, dass tatsächliche Ereignisse, die die Funktionsfähigkeit wesentlicher Dienste beeinträchtigt haben, auch als empirische Basisdaten für die Risikobewertung genutzt werden können.

Diese Risikoanalyse basiert nicht nur auf Modellen und Szenarien, sondern auch auf realen Störungsdaten. Das ermöglicht ein lernendes, datenbasiertes Risikomanagement nach dem Prinzip des „Feedback Loops“, wie es auch die ISO 31000 fordert.

Der Bundesminister für Inneres ist verpflichtet, die relevanten Elemente der Risikoanalyse an jene Organisationen zu übermitteln, die gemäß § 11 RKEG als kritische Einrichtung identifiziert wurden. Dabei müssen alle weitergegebenen Informationen anonymisiert werden, um sicherheitsrelevante Details oder personenbezogene Daten zu schützen.

---

<sup>18</sup> „Sicherheitsvorfall“ iSd § 3 Z3 RKEG: ein Ereignis, das die Erbringung eines wesentlichen Dienstes erheblich stört oder stören könnte, einschließlich einer Beeinträchtigung der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit.

<sup>19</sup> Ein Kaskadeneffekt (cascading effect) bezeichnet in der Risiko- und Resilienzforschung den Prozess aufeinanderfolgender Ausfälle oder Störungen, bei dem eine primäre Störung in einem System durch Interdependenzen weitere Störungen in anderen Systemen oder Sektoren auslöst. Diese Übertragung kann physischer, technologischer, organisatorischer oder sozialer Natur sein - Pescaroli, G./Alexander, D. (2018).

<sup>20</sup> Linkov, I./Trump, B.D. (2019).

Dieser Ansatz stellt die operative Rückkopplung zwischen staatlicher und betrieblicher Ebene sicher. Die Ergebnisse dieser Risikoanalyse (Makroebene) fließen zurück an kritischen Einrichtungen (Mikroebene), die ihre unternehmensspezifischen Risikoanalysen darauf aufbauen, wie auch im § 14 RKEG gefordert wird.

## 2.4 Europäische Rechtsgrundlagen sektoraler Risikoanalysen

Diese Risikoanalyse ist nicht isoliert zu betrachten, sondern Teil eines europäisch integrierten Systems von Risiko- und Resilienzvorgaben. Gemäß § 10 Abs. 2 Z 2 RKEG hat der Bundesminister für Inneres bei der Erstellung dieser Risikoanalyse jene Risikoanalysen zu berücksichtigen, die im Einklang mit einschlägigen sektorspezifischen EU-Rechtsakten durchgeführt werden. Diese Rechtsakte konkretisieren, wie Risiken in besonders sensiblen Infrastrukturbereichen, insbesondere Energie, Industrie und Wasserwirtschaft, zu identifizieren, zu bewerten und zu managen sind.<sup>21</sup>

Ziel dieser Integration ist die Harmonisierung nationaler Risikoanalysen mit europäischen Standards, um sicherzustellen, dass Österreichs Resilienzplanung kohärent in die europäische Sicherheitsarchitektur eingebettet wird. Die Berücksichtigung dieser EU-Vorgaben fördert die Vergleichbarkeit von Risikoergebnissen, erleichtert die grenzüberschreitende Kooperation und ermöglicht eine gemeinsame Bewertung sektorübergreifender Gefahren im Sinne des europäischen All-Gefahren-Ansatzes.<sup>22</sup>

Im Folgenden werden die im § 10 Abs. 2 Z 2 RKEG ausdrücklich genannten EU-Rechtsakte dargestellt, die als rechtliche und methodische Bezugsrahmen für die sektorale Risikoanalyse dienen. Sie bilden die Grundlage für die Einbindung europäischer Risikodaten, sektoraler Vorsorgepläne und Berichtspflichten in die nationale Risikoanalyse gemäß RKEG und stellen somit eine Schnittstelle zwischen europäischem Recht, nationaler Umsetzung und praktischem Risikomanagement dar.

### **Artikel 6 Absatz 1 des Beschlusses Nr. 1313/2013/EU über ein Katastrophenschutzverfahren der Union**

Der Beschluss Nr. 1313/2013/EU des Europäischen Parlaments und des Rates bildet den Rechtsrahmen für das Katastrophenschutzverfahren der Europäischen Union (Union Civil

---

<sup>21</sup> European Commission (2021).

<sup>22</sup> OECD (2018).

Protection Mechanism, UCPM). Sein Ziel ist es, die Zusammenarbeit zwischen der Union und den Mitgliedstaaten im Bereich des Katastrophenschutzes, der Prävention, Vorbereitung und Reaktion auf Katastrophen zu stärken. Er führt erstmals eine verbindliche Verpflichtung zu nationalen Risikoanalysen ein, um Katastrophenprävention auf eine gemeinsame Wissensbasis zu stellen. Artikel 6 bildet dabei den Kern des präventiven Risikomanagements und ist unmittelbar relevant für die nationale Risikoanalyse gemäß § 10 RKEG.

Artikel 6 des Beschlusses Nr. 1313/2013/EU lautet wie folgt:

*„Artikel 6 Risikomanagement*

*Zur Förderung eines wirksamen und kohärenten Ansatzes bei der Katastrophenprävention und -vorsorge durch den Austausch nicht sensibler Informationen, namentlich Informationen, deren Preisgabe nicht den wesentlichen Sicherheitsinteressen der Mitgliedstaaten widersprechen würde, und durch den Austausch bewährter Vorgehensweisen im Rahmen des Unionsverfahrens gehen die Mitgliedstaaten wie folgt vor:*

*a) Sie erstellen Risikobewertungen auf nationaler oder geeigneter subnationaler Ebene und stellen der Kommission bis zum 22. Dezember 2015 und danach alle drei Jahre eine Zusammenfassung der einschlägigen Punkte dieser Risikobewertungen zur Verfügung;*

*b) sie entwickeln und verfeinern ihre Katastrophenrisikomanagementplanung auf nationaler oder geeigneter subnationaler Ebene;*

*c) sie stellen der Kommission nach der endgültigen Erarbeitung der einschlägigen Leitlinien gemäß Artikel 5 Absatz 1 Buchstabe f alle drei Jahre und jedes Mal, wenn bedeutende Änderungen vorliegen, die Bewertung ihrer Risikomanagementfähigkeit auf nationaler oder geeigneter subnationaler Ebene zur Verfügung, und*

*d) sie nehmen auf freiwilliger Basis an gegenseitigen Begutachtungen der Bewertung ihrer Risikomanagementfähigkeit teil.“<sup>23</sup>*

Der Artikel beschreibt vier konkrete Handlungsfelder (lit. a bis d), die jeder Mitgliedstaat umzusetzen hat. Lit. a verpflichtet die Mitgliedstaaten zur regelmäßigen Erstellung nationaler Risikobewertungen und zur Übermittlung einer Zusammenfassung an die Europäische

---

<sup>23</sup> Beschluss (EU) 1313/2013 des Europäischen Parlaments und des Rates vom 17. Dezember 2013 über ein Katastrophenschutzverfahren der Union, ABl. Nr. L 347 vom 20.12.2013.

Kommission. Die Fristsetzung, erstmalig bis 22. Dezember 2015, danach alle drei Jahre, begründet einen fortlaufenden Berichtszyklus. Ziel ist die Vergleichbarkeit der nationalen Gefährdungslagen, die Identifikation gemeinsamer Gefahren bzw. Risiken und die Förderung der europäischen Katastrophenresilienz. In der Vergangenheit wurde diese Verpflichtung durch die *nationale Risikobewertung und Bewertung der Risikomanagementfähigkeiten 2023 (Mitteilung der Republik Österreich gemäß Artikel 6 des Katastrophenschutzverfahrens der Union)*<sup>24</sup> und in weiterer Form auch durch § 10 Abs. 1 RKEG umgesetzt, der den Bundesminister für Inneres zur Erstellung und regelmäßigen Adaptierung, längstens nach vier Jahren, der nationalen Risikoanalyse gemäß RKEG verpflichtet.

Die Bestimmung in lit. b verlangt, dass auf Grundlage der Risikoanalyse strategische Planungen und Vorsorgemaßnahmen entwickelt werden. Dazu zählen bspw. Frühwarnsysteme, Notfallpläne, Redundanzmaßnahmen, Ressourcenplanung und Kommunikationsprotokolle. Damit rückt diese Regelung die Transformation von Wissen in Handeln in den Mittelpunkt des europäischen Risikomanagements, ebenso ein Kernelement der ISO 31000. Diese Risikoanalyse dient somit als Planungsgrundlage für operative Krisenbewältigung bei kritischen Einrichtungen.

In lit. c verpflichtet die EU die Mitgliedstaaten, regelmäßig die eigene Leistungs- und Reaktionsfähigkeit zu bewerten. Diese „Capability Assessments“ umfassen bspw. institutionelle und gesetzliche Strukturen, verfügbare Ressourcen und Einsatzkräfte, technische und wissenschaftliche Kompetenzen sowie Koordinations- und Kommunikationsmechanismen. Diese Selbstbewertung bildet die Grundlage für gegenseitiges Lernen und Peer Reviews zwischen Staaten.<sup>25</sup>

Lit. d fördert den freiwilligen Mechanismus des europäischen Erfahrungsaustauschs und ermöglicht es den Mitgliedstaaten, ihre Systeme extern evaluieren zu lassen.

Aus Sicht der Forschung gilt Artikel 6 als Grundpfeiler einer europäischen Risikogovernance. Er operationalisiert das Prinzip des integrierten Risikomanagements (IRM) und bildet den institutionellen Rahmen für Multi-Level-Resilienz.<sup>26</sup>

## **Verordnung (EU) 2019/941 – Risikovorsorge im Elektrizitätssektor**

---

<sup>24</sup> BMI (2024b)

<sup>25</sup> Linkov, I. / Trump, B.D. (2019).

<sup>26</sup> Pescaroli, G. / Alexander, D. (2018).

Die Verordnung (EU) 2019/941 über die Risikovorsorge im Elektrizitätssektor<sup>27</sup> ist ein zentraler Bestandteil des sogenannten „*Clean Energy Package*“ der Europäischen Union. Ihr Hauptziel besteht darin, die Resilienz und Versorgungssicherheit des europäischen Stromsystems zu stärken, indem Mitgliedstaaten verpflichtet werden, koordinierte Risikoanalysen und Krisenvorsorgepläne im Elektrizitätssektor zu erstellen.

Die Verordnung stellt sicher, dass die Vorbereitung auf Stromversorgungskrisen systematisch, methodisch und unionsweit abgestimmt erfolgt. Damit ist sie unmittelbar relevant für diese Risikoanalyse, insbesondere im Hinblick auf kritische Einrichtungen im Energiesektor. Zusätzlich legt sie den rechtlichen Rahmen für Prävention, Vorbereitung und Krisenreaktion im Elektrizitätssektor fest. Sie gilt für alle Mitgliedstaaten und betrifft insbesondere Übertragungsnetzbetreiber, Marktteilnehmer, Regulierungsbehörden und zuständige Ministerien.<sup>28</sup>

Die Kernelemente sind in Artikel 5 bis 14 geregelt und umfassen Pflichten, wie die gemeinsame Methodik für Risikoanalysen (Art. 5), die Erstellung nationaler Risikovorsorgepläne (Art. 10 und 11), die regionale Koordination und den Informationsaustausch (Art. 12 und 13) sowie die Krisenbewältigung und Berichterstattung (Art. 15 bis 17).

Der § 10 Abs. 2 Z 2 RKEG verpflichtet den Bundesminister für Inneres, die auf Grundlage dieser Verordnung durchgeführten Risikoanalysen explizit in diese Risikoanalyse einzubeziehen. Dadurch werden bspw. sektorale Energiestudien, Netzstabilitätsanalysen und Versorgungssicherheitsbewertungen zu integralen Bestandteilen der staatlichen Gesamtbewertung. In der Praxis bedeutet dies, dass der österreichische Energiesektor regelmäßig Daten und Risikoanalysen in diese Risikoanalyse einbringt.

Die Verordnung gilt als Best-Practice-Modell für sektorale Resilienzpolitik. Sie überträgt das Prinzip des Risikomanagementzyklus aus ISO 31000 auf den Energiesektor und institutionalisiert eine strukturierte, mehrstufige Kooperation zwischen Staaten und kritischer Infrastruktur.<sup>29</sup>

---

<sup>27</sup> Verordnung (EU) 2019/941 des Europäischen Parlaments und des Rates vom 5. Juni 2019 über Risikovorsorge im Elektrizitätssektor und zur Aufhebung der Richtlinie 2005/89/EG, ABl. Nr. L 158 vom 14.6.2019.

<sup>28</sup> Monie, S. / Gustafsson, M. / Önnared, S. / Guruvita, K. M. (2025).

<sup>29</sup> Baldursson, F. M. / Banet, C. / Chyong, C. K. (2023).

## **Verordnung (EU) 2017/1938 über Maßnahmen zur Gewährleistung der sicheren Gasversorgung**

Diese Verordnung des Europäischen Parlaments und des Rates vom 25. Oktober 2017 bildet das aktuelle Fundament der europäischen Gasversorgungssicherheitspolitik. Ihr zentrales Ziel ist es, eine unterbrechungsfreie Gasversorgung für alle Mitgliedstaaten der Europäischen Union sicherzustellen, insbesondere bei außergewöhnlich hoher Nachfrage oder bei Ausfällen von Lieferquellen<sup>30</sup>.

Die Verordnung gilt für Erdgasunternehmen, Mitgliedstaaten, Regulierungsbehörden sowie Übertragungsnetzbetreiber und bezieht sich auf die Planung, Vorsorge und Bewältigung von Versorgungsstörungen. Risiken sollen auf nationaler, regionaler und Unionsebene systematisch analysiert werden, um Vorsorgemaßnahmen zu planen und im Krisenfall koordiniert reagieren zu können.

Gemäß Art. 7-9 muss jeder Mitgliedstaat, alle vier Jahre eine nationale Risikoanalyse der Gasversorgung erstellen. Diese muss mindestens die Identifikation der Gefahren und Bedrohungen für das Gasnetz, die Bewertung der Abhängigkeiten von Importen und Transitländern und die Auswirkungen sektorübergreifender Störungen beinhalten. Auf Basis dieser Analyse müssen die Staaten Präventionsmaßnahmen entwickeln und in einem Präventionsplan veröffentlichen.

Zusätzlich definiert die Verordnung, im Fall einer tatsächlichen Gaskrise ein dreistufiges Krisenmanagementsystem, darunter ist eine Frühwarnstufe, eine Alarmstufe und eine Notfallstufe zu verstehen.

Mitgliedstaaten müssen in allen Phasen ihre nationalen Notfallpläne aktivieren und untereinander Informationen austauschen. Besonders wichtig ist der Solidaritätsmechanismus im Art. 13, der vorsieht, dass Mitgliedstaaten benachbarte Staaten unterstützen, wenn die Gasversorgung gefährdet ist. Dieses Prinzip der gegenseitigen Resilienz entspricht dem in der Literatur beschriebenen Ansatz der *shared resilience*<sup>31</sup>.

---

<sup>30</sup> Europäische Union (2017): Verordnung (EU) 2017/1938 des Europäischen Parlaments und des Rates vom 25. Oktober 2017 über Maßnahmen zur Gewährleistung der sicheren Gasversorgung und zur Aufhebung der Verordnung (EU) Nr. 994/2010

<sup>31</sup> Pescaroli, G., & Alexander, D. (2018).

Die Verordnung definiert vorgegebene Kooperationsregionen, innerhalb derer Mitgliedstaaten ihre Risikoanalysen und Präventionspläne gemeinsam abstimmen müssen. Österreich ist in mehreren Risikogruppen vertreten<sup>32</sup>, meist mit Deutschland, Tschechien, der Slowakei, Ungarn, Polen, Slowenien und Kroatien. Diese sektorübergreifende Zusammenarbeit zielt darauf ab, grenzüberschreitende Kaskadeneffekte zu minimieren<sup>33</sup>.

Wissenschaftlich wird die Verordnung (EU) 2017/1938 als wichtiger Schritt hin zu einer Resilienzorientierung der Energiepolitik gewertet. Sie operationalisiert erstmals das Konzept des integrierten Risiko- und Krisenmanagements im europäischen Gasmarkt und verknüpft rechtliche Verpflichtungen mit Resilienztheoretischen Ansätzen<sup>34</sup>. Nach *Baldursson et al.* ist diese Verordnung ein zentrales Element der „European Energy Resilience Governance“, weil sie transnationale Abhängigkeiten in konkrete Handlungsprozesse übersetzt<sup>35</sup>.

### **Richtlinie 2012/18/EU (Seveso III) – Beherrschung der Gefahren schwerer Unfälle mit gefährlichen Stoffen**

Diese EU-Richtlinie (Seveso III) ersetzt die vorherige Seveso II (96/82/EG) und bildet das zentrale europäische Regelwerk zur Verhütung schwerer Industrieunfälle mit gefährlichen Stoffen. Sie dient der Harmonisierung von Sicherheitsstandards, Meldepflichten und Risikobewertungen innerhalb der EU. Ihr Hauptziel ist die Vermeidung und Begrenzung der Auswirkungen schwerer Unfälle auf Mensch und Umwelt<sup>36</sup>.

Die Richtlinie gilt für Betriebe, die bestimmte Mengen gefährlicher Stoffe bei Lagerung, Transport, Verarbeitung etc. überschreiten. Sie verpflichtet Betreiber von solchen Betrieben und Mitgliedstaaten zu umfassenden Sicherheitsmaßnahmen, wie Implementierung eines funktionierenden Sicherheitsmanagements und einer Grundsaterklärung zur Verhütung schwerer Unfälle. Diese müssen dokumentiert, überprüfbar und regelmäßig evaluiert werden. Zusätzlich müssen Sicherheitsberichte vorlegen werden, welche Gefahrenquellen, mögliche Unfallverläufe und Schutzmaßnahmen enthalten. Ergänzend sind interne und externe Notfallpläne zu erstellen und regelmäßig zu testen. Die Mitgliedstaaten müssen Seveso-Anlagen in die nationale Raumplanung integrieren (bspw. Sicherheitsabstände oder

---

<sup>32</sup> „Gasversorgung Ost“, „Gasversorgung Nordafrika“, „Gasversorgung Südost“ und „Südlicher Gaskorridor“.

<sup>33</sup> Pescaroli, G.; Trump, B. D.; Linkov, I.; Alexander, D. (2024).

<sup>34</sup> Monie, S.; Gustafsson, M.; Önnared, S.; Guruvita, K. M. (2025).

<sup>35</sup> E Baldursson, F. M., Banet, C., & Chyong, C. K. (2023).

<sup>36</sup> Europäische Union (2012): Richtlinie 2012/18/EU über die Beherrschung der Gefahren schwerer Unfälle mit gefährlichen Stoffen.

Nutzungskontrolle) und die Öffentlichkeit aktiv einbeziehen. Betriebe sind verpflichtet, Unfälle zu melden, Ursachen zu analysieren und die Ergebnisse für systemisches Lernen zu teilen. Diese Daten fließen in das EU-Seveso-Inspektionsnetzwerk.

Neuere Studien zeigen, dass Seveso III zunehmend als Resilienzrahmen verstanden wird, weg von reiner Unfallprävention hin zu systemischem Risikomanagement und moderne Quantitative Risk Assessments (QRA) bildet<sup>37</sup>.

### **Richtlinie 2007/60/EG – Bewertung und Management von Hochwasserrisiken (EU-Hochwasserrichtlinie)**

Die EU-Hochwasserrichtlinie 2007/60/EG wurde 2007 als Reaktion auf eine Reihe schwerer Überschwemmungen in Mitteleuropa erlassen.

Ihr Ziel ist es, Hochwasserrisiken zu bewerten, zu reduzieren und zu managen, indem Mitgliedstaaten einen standardisierten dreistufigen Zyklus durchführen, welcher die vorläufige Bewertung, Gefahren- und Risikokarten und Hochwasserrisikomanagementpläne enthält.

Sie gilt als Eckpfeiler der europäischen Klimaanpassungs- und Katastrophenschutzpolitik und ist unmittelbar relevant für diese Risikoanalyse gemäß RKEG, da klimawandelbedingte Risiken hier systematisch abgebildet werden müssen<sup>38</sup>. Die Mitgliedstaaten müssen alle sechs Jahre eine vorläufige Bewertung durchführen, um Gebiete mit potenziell signifikantem Hochwasserrisiko zu bestimmen. Für jedes dieser Gebiete werden Karten erstellt, die Überflutungsflächen, Wassertiefen, Fließgeschwindigkeiten und potenzielle Schadensauswirkungen darstellen. Diese Daten bilden die Grundlage für Schadens- und Resilienzbewertung. Zusätzlich müssen Hochwasserrisikomanagementpläne erarbeitet werden, welche präventive, schützende und vorbereitende Maßnahmen definieren<sup>39</sup>. Sie sind regelmäßig zu aktualisieren und müssen mit anderen Richtlinien bspw. der EU-Wasserrahmenrichtlinie<sup>40</sup> abgestimmt werden.

---

<sup>37</sup> Akel, N. J.; Simone, F.; Stefana, E.; Ansaldi, S. M.; Agnello, P.; Vallerotonda, M. R.; Di Gravio, G.; Patriarca, R. (2025).

<sup>38</sup> Dráb, A.; Říha, J. (2010).

<sup>39</sup> Europäische Union (2007): Richtlinie 2007/60/EG über die Bewertung und das Management von Hochwasserrisiken.

<sup>40</sup> Richtlinie 2000/60/EG des Europäischen Parlaments und des Rates vom 23. Oktober 2000 zur Schaffung eines Ordnungsrahmens für Maßnahmen der Gemeinschaft im Bereich der Wasserpolitik

## 2.5 Begriffe und Definitionen

Dabei handelt es sich um die Begriffe und ihre Definitionen gemäß § 3 RKEG.

- **„kritische Einrichtung“**: eine öffentliche oder private Einrichtung, die in Anwendung des § 11 RKEG vom Bundesminister für Inneres als solche eingestuft wurde.
- **„Resilienz“**: die Fähigkeit einer kritischen Einrichtung, einen Sicherheitsvorfall zu verhindern, sich davor zu schützen, einen solchen abzuwehren, darauf zu reagieren, die Folgen eines solchen Vorfalls zu begrenzen, einen Sicherheitsvorfall zu bewältigen oder sich von einem solchen Vorfall zu erholen;
- **„Sicherheitsvorfall“**: ein Ereignis, das die Erbringung eines wesentlichen Dienstes erheblich stört oder stören könnte, einschließlich einer Beeinträchtigung der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit;
- **„Beinahe-Sicherheitsvorfall“**: ein Ereignis mit dem Potenzial, einen Sicherheitsvorfall hervorzurufen, dessen Eintritt aber noch rechtzeitig verhindert werden konnte oder der aus sonstigen Gründen nicht eingetreten ist;
- **„kritische Infrastruktur“**: Objekte, Anlagen, Ausrüstungen, Netze, Systeme oder Teile eines Objekts, einer Anlage, einer Ausrüstung, eines Netzes oder eines Systems, die für die Erbringung eines wesentlichen Dienstes erforderlich sind;
- **„wesentlicher Dienst“**: ein Dienst, der in der Delegierten Verordnung (EU) 2023/2450 zur Ergänzung der Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates durch eine Liste wesentlicher Dienste, ABl. Nr. L 2023/2450 vom 30.10.2023, festgelegt wurde; darüber hinaus allfällige weitere aufgrund einer Verordnung des Bundesministers für Inneres festgelegte Dienste, die für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, wichtiger wirtschaftlicher Tätigkeiten, der öffentlichen Gesundheit und Sicherheit oder die Erhaltung der Umwelt von erheblicher Bedeutung sind und von einer Einrichtung der im Anhang der RKE-Richtlinie angeführten Kategorien in den gelisteten Sektoren und Teilsektoren erbracht werden;
- **„Risiko“**: das Potenzial für Verluste oder Störungen, die durch einen Sicherheitsvorfall verursacht werden, das als eine Kombination des Ausmaßes eines solchen Verlusts

oder einer solchen Störung und der Wahrscheinlichkeit des Eintretens des Sicherheitsvorfalls zum Ausdruck gebracht wird;

- **„Risikoanalyse“**: der gesamte Prozess zur Bestimmung der Art und des Ausmaßes eines Risikos, bei dem potenzielle Bedrohungen, Schwachstellen oder Gefahren für kritische Einrichtungen, die zu einem Sicherheitsvorfall führen können, ermittelt und analysiert und die durch den Sicherheitsvorfall verursachten potenziellen Verluste oder Störungen bei der Erbringung eines wesentlichen Dienstes samt Eintrittswahrscheinlichkeit bewertet werden; im Zuge dieser Risikoanalyse werden sämtliche aus natürlichen Ursachen herrührenden oder vom Menschen verursachten Risiken, die zu einem Sicherheitsvorfall führen können, berücksichtigt;
- **„Mitgliedstaat“**: jeder Staat, der Vertragspartei des Vertrags über die Europäische Union in der Fassung BGBl. III Nr. 132/2009 ist;
- **„Drittstaat“**: jeder Staat, der nicht Vertragspartei des Vertrags über die Europäische Union in der Fassung BGBl. III Nr. 132/2009 ist;
- **„Einrichtung“**: eine natürliche oder juristische Person, eine eingetragene Personengesellschaft oder eine Stelle der öffentlichen Verwaltung;
- **„Resilienzplan“**: ein Dokument, in dem die geeigneten und verhältnismäßigen technischen, sicherheitsbezogenen und organisatorischen Maßnahmen zur Gewährleistung der Resilienz nachvollziehbar dargelegt werden;
- **„Audit“**: eine systematische und unabhängige Überprüfung der Einhaltung der Verpflichtungen gemäß den §§ 14 und 15 RKEG, insbesondere durch Bewertungsbesuche, samt Dokumentation der Ergebnisse in einem Prüfbericht durch Resilienzauditoren (§ 21 RKEG).

# 3 Kontext Österreich

## Anforderungen gemäß ÖNORM D 4901 Normpunkt 4

Das Verständnis des organisatorischen und externen Kontextes bildet gemäß ISO 31000 und Normpunkt 4 der ÖNORM D 4901 den Ausgangspunkt jedes Risikomanagementprozesses. Im Rahmen dieser Risikoanalyse umfasst dieser Kontext alle politischen, wirtschaftlichen und gesellschaftlichen Rahmenbedingungen, die das gesamte Risiko- und Resilienzprofil der kritischen Einrichtungen beeinflussen. Ziel dieses Kapitels ist es, jene übergeordneten Einflussfaktoren zu beschreiben, die die Durchführung, Bewertung und Wirksamkeit von Risikoanalysen maßgeblich prägen. Dazu zählen die staatlichen und regulatorischen Strukturen des österreichischen Krisen- und Sicherheitsmanagements, wirtschaftliche Interdependenzen innerhalb zentraler Versorgungssektoren, gesellschaftliche Erwartungshaltungen an Versorgungssicherheit, die topografische und klimatische Ausgangslage sowie die Beziehungen zu den Stakeholdern. Ergänzend werden historische Risikoerfahrungen und nationale Gefahrenanalysen herangezogen, um ein konsistentes Bild der Risikolandschaft Österreichs zu zeichnen. Dieses Kapitel schafft damit die analytische Grundlage, auf der die Risikoidentifikation und -bewertung in den folgenden Kapiteln aufbauen.

### 3.1 Politischer, wirtschaftlicher und gesellschaftlicher Kontext

Der politische, wirtschaftliche und gesellschaftliche Kontext definiert jene Rahmenbedingungen, unter denen diese Risikoanalysen durchgeführt wird. Nach der ÖNORM D 4901 und der ISO 31000 bildet die Erfassung des externen Umfelds die Grundlage jeder Risikoanalyse. Im Sinne des RKEG ist dieser Kontext nicht nur beschreibend, sondern handlungsleitend und bestimmt, welche Gefährdungen für die Versorgungssicherheit relevant sind, welche Akteure eingebunden werden müssen und in welchem rechtlich-politischen System die Resilienzplanung verankert ist.

#### 3.1.1 Politischer Kontext

Österreich verfügt über ein ausgeprägtes Mehr-Ebenen-Governance-System, in dem sicherheits- und infrastrukturelevante Kompetenzen zwischen Bund, Ländern und Gemeinden

geteilt sind.<sup>41</sup> Das Gesetz verpflichtet den Bundesminister für Inneres zur Erstellung einer nationalen Risikoanalyse<sup>42</sup> und kritische Einrichtungen zur Durchführung eigener Risikoanalysen<sup>43</sup> sowie zur Ergreifung entsprechender Resilienzmaßnahmen.<sup>44</sup>

Der politische Handlungsrahmen wird flankiert, bspw. von der Österreichischen Sicherheitsstrategie 2024<sup>45</sup>, der Österreichischen Strategie zur Anpassung an den Klimawandel<sup>46</sup>, der Österreichischen Cybersicherheitsstrategie 2021<sup>47</sup> und dem Leitfaden des Staatlichen Krisen- und Katastrophenmanagements (SKKM)<sup>48</sup>. Diese Dokumente betonen die zunehmende Verknüpfung von physischer und digitaler Sicherheit, die Notwendigkeit präventiver Maßnahmen sowie die Bedeutung resilienter Wertschöpfungsnetze.

Zusätzlich müssen Risikoanalysen, welche dezidiert in § 10 RKEG aufgelistet sind, bspw. die allgemeine Risikoanalyse gemäß Art. 6 Abs. 1 des Beschlusses Nr. 1313/2013/EU über ein Katastrophenschutzverfahren oder gemäß Verordnung (EU) 2019/941 über die Risikovor-sorge im Elektrizitätssektor und zur Aufhebung der Richtlinie 2005/89/EG, sowie anderer Risikoanalysen, die im Einklang mit den Anforderungen einschlägiger sektorspezifischer Rechtsakte der Union durchgeführt werden, berücksichtigt werden.

Die politische Steuerung orientiert sich zunehmend an Prinzipien der Risikogovernance. Staatliche Steuerung erfolgt demnach evidenzbasiert, partizipativ und sektorübergreifend.<sup>49</sup> Verwaltungswissenschaftliche Analysen bestätigen, dass Österreichs föderale Struktur sowohl Stärken (regionale Anpassungsfähigkeit) als auch Schwächen (Koordinationsauf-wand) im Krisenmanagement aufweist<sup>50</sup>. Für kritische Einrichtungen bedeutet dies, dass Risikoanalysen den föderalen Handlungsspielraum und die interinstitutionellen Schnittstellen ausdrücklich berücksichtigen müssen.

---

<sup>41</sup> Institut für Föderalismus (2023).

<sup>42</sup> § 10 RKEG.

<sup>43</sup> § 14 RKEG.

<sup>44</sup> § 15 RKEG.

<sup>45</sup> BKA (2024).

<sup>46</sup> BMK (2024).

<sup>47</sup> BKA (2021).

<sup>48</sup> BMI (2018).

<sup>49</sup> Renn, O. (2020).

<sup>50</sup> Schulte, Y. / Schönfeld, M. / Schütte, P. M. / Friedrich, F. (2024).

### 3.1.2 Wirtschaftlicher Kontext

Die österreichische Volkswirtschaft ist stark internationalisiert und eng in den EU-Binnenmarkt eingebunden. Mehr als Zweidrittel der Exporte gehen in EU-Mitgliedstaaten, womit Österreich besonders von europäischen Liefer- und Energieflüssen abhängig ist.<sup>51</sup> Gleichzeitig ist die Energie-, Logistik- und Informationsinfrastruktur über technische Netze eng mit Nachbarstaaten gekoppelt.<sup>52</sup> Laut der Statistikbroschüre der E-Control gilt Österreichs Energie- und Transportinfrastruktur als „hochgradig systemisch“, da Störungen in einem Teilbereich (bspw. Stromnetz oder digitale Steuerung) Kaskadeneffekte in anderen Sektoren auslösen können.

Eine ökonomische Analyse des Österreichischen Instituts für Wirtschaftsforschung (WIFO)<sup>53</sup> hebt hervor, dass geopolitische Abhängigkeiten, insbesondere im Energiesektor und Störungen globaler Lieferketten zentrale Resilienzfaktoren darstellen. Im Rahmen dieser Risikoanalyse müssen somit physische, ökonomische und strategische Herausforderungen gleichermaßen erfasst werden.

Darüber hinaus weisen aktuelle technische Studien auf wachsende technologische Abhängigkeiten hin, etwa von Software-, Cloud- und Kommunikationsanbietern. Die Integration digitaler Systeme führt zu neuen Bedrohungslagen, die an der Schnittstelle zwischen Cyber- und physischer Resilienz adressiert werden müssen.<sup>54</sup>

### 3.1.3 Gesellschaftlicher Kontext

Österreich weist ein hohes Maß an gesellschaftlicher Stabilität, sozialem Vertrauen und institutioneller Dichte auf. Dennoch verändern Digitalisierung, Urbanisierung und demografischer Wandel die gesellschaftliche Risikolandschaft deutlich.<sup>55</sup>

Oft entscheidet gesellschaftliche Akzeptanz über die Wirksamkeit sicherheits- und resilienzpoltischer Maßnahmen. Besonders wichtig sind transparente Kommunikations- und Beteiligungsprozesse zwischen Behörden, kritischen Einrichtungen und der Bevölkerung. Das

---

<sup>51</sup> Europäische Kommission (2024).

<sup>52</sup> E-Control (2023).

<sup>53</sup> WIFO (2024).

<sup>54</sup> BMFWF (2025).

<sup>55</sup> IHS (2024).

RKEG greift die Themen der Meldepflichten gemäß § 17 RKEG und der jährlichen Berichterstattung durch den Bundesminister für Inneres auf, um institutionelles Vertrauen und Nachvollziehbarkeit zu fördern.<sup>56</sup>

Versorgungsstörungen, etwa im Energie- oder Gesundheitssektor dürfen nicht nur als funktionale, sondern müssen auch als politische Krisen wahrgenommen werden. Für diese Risikoanalyse bedeutet dies, dass neben technischen und wirtschaftlichen Faktoren auch sozialpsychologische Risikotreiber einzubeziehen sind.<sup>57</sup>

Der österreichische Kontext ist geprägt von stabilen politischen Institutionen, einem hochgradig vernetzten Wirtschaftssystem und einer risikobewussten Gesellschaft. Diese Kombination schafft günstige Voraussetzungen für ein koordiniertes Risikomanagement, erhöht jedoch die systemische Komplexität und den Kommunikationsbedarf. Risikoanalysen kritischer Einrichtungen müssen daher interdisziplinär angelegt, wirtschaftlich fundiert und gesellschaftlich akzeptiert sein.

## 3.2 Geografische und ökologische Rahmenbedingungen

Österreichs geografische und ökologische Rahmenbedingungen prägen maßgeblich die Exposition kritischer Einrichtungen gegenüber Naturgefahren und klimabedingten Risiken. Im Sinne der ISO 31000 und ÖNORM D 4901 müssen Risikoanalysen den physischen Standortkontext, natürliche Gefährdungslagen und ökologische Veränderungsprozesse systematisch berücksichtigen, um ein realistisches Risikoprofil zu erstellen. Der All-Gefahren-Ansatz verpflichtet den Bundesminister für Inneres, sowie kritische Einrichtungen ausdrücklich, sowohl von der Natur verursachte als auch anthropogene bzw. intentionale sowie technische Gefahren in ihre Analysen einzubeziehen.

Österreich ist durch eine stark differenzierte Topografie geprägt: Rund 63 % der Landesfläche ist Alpengebiet,<sup>58</sup> während die bevölkerungsreichsten Gebiete in den Tälern und im Donaunraum liegen. Diese Siedlungsstruktur führt dazu, dass wesentliche Teile der kritischen

---

<sup>56</sup> Petersen, L. / Fallou, L. / Reilly, P. / Serafinelli, E. (2017).

<sup>57</sup> Boin, A. / Hart, P. / Stern, E. / Sundelius, B. (2005).

<sup>58</sup> Statistik Austria (2024).

Infrastruktur Österreichs, wie etwa die Energieversorgung, Verkehrskorridore und Kommunikationsleitungen in räumlich konzentrierten Korridoren verlaufen.<sup>59</sup>

Die räumliche Verdichtung in Ballungsräumen erhöht die Anfälligkeit gegenüber kumulativen Ereignissen, wie Stromausfällen oder Hochwasserfolgen in Infrastrukturbereichen mit hoher Netzabhängigkeit.<sup>60</sup> Gleichzeitig bestehen in alpinen Regionen zugangs- und instandhaltungstechnische Herausforderungen, etwa durch Lawinen-, Muren- oder Felssturzgefahr. Diese topografische Dualität, im Sinne von einer hohen Dichte in urbanen Räumen und physischer Exponiertheit im Gebirge, erfordert eine raumtypische Differenzierung der Risikoanalyse.<sup>61</sup>

Klimatische Veränderungen wirken in Österreich besonders stark. Es werden signifikante Zunahmen von Extremereignissen, bspw. Hitzewellen, Starkniederschlägen, Trockenperioden und Spätfrostereignisse dokumentiert.<sup>62</sup> Diese Ereignisse können alleine auftreten oder unmittelbar aufeinander folgend, wodurch sich die Auswirkungen verstärken. Beispielhaft kann eine Trockenperiode gefolgt von einem Starkregenereignis genannt werden.

Diese klimatischen Veränderungen beeinflussen unmittelbar die Betriebssicherheit und Planung kritischer Einrichtungen:

- Hitzewellen führen zu Überlastung elektrischer Netze und Kühlkapazitäten,<sup>63</sup>
- Starkregen und Hochwasser gefährden Energie-, Wasser- und Verkehrsinfrastrukturen<sup>64</sup>
- Trockenheit wirkt sich auf Wasserkraftnutzung und Kühlwasserversorgung aus<sup>65</sup>

Im Zuge des European Climate Risk Assessment 2024<sup>66</sup> wird Österreich als Land mit hoher Klimarisikokonzentration in Gebirgs- und Flussregionen eingestuft. Für das Bundesministe-

---

<sup>59</sup> ÖROK (2023).

<sup>60</sup> EEA (2020).

<sup>61</sup> Umweltbundesamt (2023).

<sup>62</sup> BMK (2024a).

<sup>63</sup> European Environment Agency (2017).

<sup>64</sup> Thaler, T. / Hartmann, T. (2016).

<sup>65</sup> Umweltbundesamt (2023).

<sup>66</sup> European Environment Agency (2024).

rium für Inneres und die kritischen Einrichtungen ergibt sich daraus die Notwendigkeit, klimawandelbedingte Stressoren als wiederkehrende und nicht mehr als Ausnahmeereignisse zu behandeln.

Österreich gehört zu den am stärksten naturgefahren dynamischen Ländern Mitteleuropas. Neben hydrologischen Risiken bestehen erhebliche Expositionen gegenüber Hochwasser, Hangrutschungen, Lawinen und Stürmen.<sup>67</sup>

Für diese Risikoanalyse ist die Integration geowissenschaftlicher Gefahrenkarten obligatorisch. Der nationale Gefahrenzonenplan (GZP)<sup>68</sup>, der Leitfaden für Risikomanagement im Katastrophenmanagement<sup>69</sup>, sowie die rechtlichen und organisatorischen Grundlagen des Staatliches Krisen- und Katastrophenschutzmanagement<sup>70</sup> bieten behördlich anerkannte Grundlagen.

Die Kombination aus alpiner Topografie, hydrologischer Dichte und zunehmenden Extremereignissen kann zu einer Kaskade multipler Risiken führen, bspw. wenn Starkregen Hangrutschungen auslöst und gleichzeitig Versorgungsleitungen beschädigt.<sup>71</sup>

Darüber hinaus spielen ökologische Degradationsprozesse, etwa Bodenversiegelung oder Waldschäden durch Borkenkäferbefall, eine wachsende Rolle für physische Resilienz.<sup>72</sup> Diese Prozesse verändern langfristig die hydrologische Retention und erhöhen somit das sekundäre Risiko infrastruktureller Ausfälle.

Die geografischen und ökologischen Rahmenbedingungen Österreichs erzeugen ein komplexes, räumlich differenziertes Risikoprofil. Während urbane Gebiete durch kritische Dichteeffekte gekennzeichnet sind, unterliegen alpine Regionen primär naturgefahren dynamischen Risiken. Klimawandel und Landnutzungsdruck verstärken diese Dynamiken zusätzlich. Für die Risikoanalyse ergibt sich daraus, dass Standort-, Klima- und Umweltfaktoren integraler Bestandteil der Risikoidentifikation und -bewertung sein müssen.

---

<sup>67</sup> European Environment Agency (2024).

<sup>68</sup> BMLUK (2025).

<sup>69</sup> BMI (2018).

<sup>70</sup> BMI (2025).

<sup>71</sup> Thaler, T. A. / Priest, S. J. / Fuchs, S. (2016).

<sup>72</sup> Bundesministerium für Landwirtschaft, Forstwirtschaft, Regionen und Wasserwirtschaft (2023).

### 3.3 Stakeholderanalyse

Die Stakeholderanalyse bildet einen wesentlichen Bestandteil des Risikomanagementprozesses gemäß ISO 31000 und der ÖNORM Reihe D 4900. Beide betonen, dass Risiken nicht isoliert, sondern im Zusammenspiel von Organisation, Akteuren und Umfeld betrachtet werden müssen. Im Kontext des RKEG dient die Stakeholderanalyse dazu, die Vielzahl an beteiligten Institutionen, Behörden, Unternehmen und Organisationen zu identifizieren und deren Rollen, Verantwortlichkeiten sowie Interaktionsbeziehungen zu bestimmen. Die Stakeholderanalyse schafft die Grundlage für wirksame Risikoanalysen im Sinne des RKEG. Sie übersetzt gesetzliche Anforderungen in eine kommunikative, partizipative und netzwerk-basierte Governance-Struktur. Nur durch frühzeitige und kontinuierliche Einbindung aller relevanten Akteure können Informationsasymmetrien vermieden, Synergien genutzt und Entscheidungen nachvollziehbar gestaltet werden.

Das Ziel der Stakeholderanalyse im Risikokontext liegt darin, Transparenz über Einfluss- und Betroffenheitsbeziehungen zu schaffen und dadurch die Wirksamkeit von Entscheidungen im Krisen- und Resilienzmanagement zu erhöhen.<sup>73</sup> Im Sicherheits- und Risikobereich kann nur durch Einbindung der folgenden Akteure ein realistisches Risikobild entstehen.<sup>74</sup>

- EU
- Bundesministerien
- Länder
- Interessenvertretungen
- kritische Einrichtungen
- Gesellschaft

Das Zusammenspiel dieser Akteure folgt einem Netzwerkmodell, wie es *Rowley*<sup>75</sup> und *Ackermann /Eden*<sup>76</sup> beschreiben. Stakeholder sind keine hierarchisch geordneten Einheiten, sondern interagierende Netzwerkknoten mit unterschiedlichen Macht- und Interessenslagen. Im Rahmen dieser Risikoanalyse wird dadurch sichtbar, welche Beziehungen kooperativ, konfliktträchtig oder kritisch für die Versorgungssicherheit in Österreich sind<sup>77</sup>.

---

<sup>73</sup> Bryson, J. M. (2004).

<sup>74</sup> Rowley, T. J. (1997).

<sup>75</sup> Rowley, T. J. (1997).

<sup>76</sup> Ackermann, F. / Eden, C. (2011).

<sup>77</sup> Ackermann, F. / Eden, C. (2011).

Eine regelmäßige Aktualisierung dieser Stakeholderanalyse ist essenziell, da Netzwerke im privat-öffentlichen Kontext durch Outsourcing, Digitalisierung und politische Reformen dynamisch sind.<sup>78</sup>

Der Faktor Vertrauen kann die Kooperationsbereitschaft von Stakeholdern entscheidend beeinflussen.<sup>79</sup> Fehlendes Vertrauen oder unklare Kommunikationsstrukturen führen hingegen zu Informationsblockaden und ineffektiven Krisenreaktionen<sup>80</sup>.

Die ÖNORM D 4901 fordert daher explizit, dass Risikomanagement „unter aktiver Einbindung relevanter Stakeholdergruppen“ zu erfolgen hat. Im Kontext des RKEG bedeutet dies, dass Einrichtungen ihre Analyseprozesse nicht nur dokumentieren, sondern auch transparent gegenüber dem Bundesminister für Inneres gestalten müssen.

### 3.4 Historische Risikoanalyse

Eine historische Risikoanalyse ist ein zentraler Bestandteil evidenzbasierten Risikomanagements. Sie dient dazu, Erkenntnisse aus vergangenen Störfällen, Krisen und Beinaheereignissen systematisch zu erfassen, zu bewerten und in künftige Präventions- und Resilienzstrategien zu überführen. Gemäß ISO 31000 ist die Analyse vergangener Ereignisse essenziell, um Wahrscheinlichkeiten, Schadensausmaße und Kaskadeneffekte realistischer einzuschätzen. Die ÖNORM D 4901 überträgt diese Forderung in den österreichischen Kontext, indem sie explizit die „Nutzung historischer Schadens-, Ereignis- und Störfalldaten“ für die Risikoidentifikation und Bewertung vorsieht.

Ziel einer historischen Risikoanalyse ist es, Erfahrungswissen in die Bewertung zukünftiger Bedrohungen zu integrieren. Frühere Ereignisse liefern Indikatoren für Schwachstellen in technischen Systemen, organisatorischen Abläufen und Kommunikationsstrukturen<sup>81</sup>.

---

<sup>78</sup> Reed, M. S. / Graves, A. / Dandy, N. / Posthumus, H. / Hubacek, K. / Morris, J. / Prell, C. / Quinn, C. H. / Stringer, L. C. (2009).

<sup>79</sup> Siegrist, M. / Cvetkovich, G. / Roth, C. (2002).

<sup>80</sup> Leach, W. D. / Pelkey, N. / Sabatier, P. A. (2002).

<sup>81</sup> Haimes, Y. Y. (2025).

Durch die systematische Auswertung von beispielsweise Störfall- oder Sicherheitsvorfallstatistiken, Audits und Katastrophenberichten kann beispielsweise eine empirisch validierte Grundlage für Eintrittswahrscheinlichkeiten geschaffen werden<sup>82</sup>.

Bereits vor Inkrafttreten des RKEG verfügte Österreich über ein etabliertes Rahmenwerk zum Schutz kritischer Infrastrukturen, das „Austrian Program for Critical Infrastructure Protection (APCIP)“<sup>83</sup>, das seit 2008 im Bundeskanzleramt (BKA) koordiniert und durch das Bundesministerium für Inneres (BMI) umgesetzt wird. Dieses Programm wurde in Zusammenhang mit dem Europäischen Programm zum Schutz Kritischer Infrastrukturen (EPCIP) der Europäischen Kommission<sup>84</sup> entwickelt und verfolgt das Ziel, nationale Schutzmaßnahmen, Risikoanalysen und sektorspezifische Strategien in ein einheitliches System einzubetten.

Das APCIP orientiert sich an denselben Prinzipien wie die ISO 31000, wie Risikoorientierung, Prävention sowie Kooperation und bildete über ein Public-Private-Partnership-Modell (PPP) die Grundlage für Informationsaustausch und Frühwarnsysteme zwischen Staat und kritischer Infrastruktur.

In den Jahren 2017, 2020 und 2022 wurden auf dieser Basis bereits mehrere nationale Risikoanalysen durchgeführt, die sektorenübergreifende Bedrohungsszenarien, bspw. Energieausfall, Cyberangriffe oder Naturgefahren umfassten. Diese Analysen erfolgten ohne ausdrücklichen gesetzlichen Auftrag, dienten jedoch als fachliche und methodische Vorläufer der Risikoanalyse nach § 10 RKEG.

Der Umgang mit Daten aus historischen Risikoanalyse umfasst mehrere methodische Schritte:<sup>85</sup>

1. Datenerhebung und -validierung: Sammlung und Prüfung von Ereignisdaten von anderen Behörden, kritischen Einrichtungen, Ländern, Versicherungen sowie Forschungseinrichtungen
2. Ereignisklassifikation: Zuordnung nach Art (technisch, natürlich, anthropogen, intentional), Ursache und Auswirkung

---

<sup>82</sup> Aven, T. (2015).

<sup>83</sup> <https://www.bmi.gv.at/505/start.aspx>. Zugriff am 20.11.2025

<sup>84</sup> <https://eur-lex.europa.eu/EN/legal-content/summary/european-programme-for-critical-infrastructure-protection.html>. Zugriff am 13.11.2025

<sup>85</sup> Cox, L. A. T. (2008).

3. Trend- und Musteranalyse: Identifikation wiederkehrender Ereignistypen oder systemischer Schwachstellen, etwa durch Häufigkeitsanalysen oder Root-Cause-Analysen<sup>86</sup>
4. Integration in aktuelle Risikoanalyse: Überführung historischer Erkenntnisse in Eintrittswahrscheinlichkeiten und Schadensausmaß.<sup>87</sup>

Diese Vorgehensweise erlaubt eine quantitativ und qualitativ abgesicherte Risikobewertung für diese Risikoanalyse, die auch die Anforderungen des RKEG erfüllt.

Ein Blick auf vergangene Ereignisse zeigt, wie historische Analysen den politischen und organisatorischen Wandel im Risikomanagement beeinflusst haben. Die Hochwasser 2002 und 2013 führten zur Etablierung des integrierten Hochwasserrisikomanagementplans und verbesserten hydrologischen Frühwarnsystems. Blackout-Szenarien in anderen Ländern veranlassten Energieversorger zu strukturierten Resilienztests und Betreiber von Unternehmen zur Erstellung von Vorsorgeplänen und Durchführung von Sicherheitsübungen. Die COVID-19 Pandemie brachte neue Erkenntnisse über Interdependenzen zwischen Gesundheits- und Versorgungsinfrastruktur und führte zur Stärkung des nationalen Koordinationsmechanismus und unter anderem zur Umsetzung des Bundes-Krisensicherheitsgesetzes (B-KSG)<sup>88</sup>. Zusätzlich wurden die gesamtstaatlichen Anstrengungen in den Bereichen SKKM und B-KSG ständig weiterentwickelt. Diese Beispiele verdeutlichen den normativen Grundsatz, dass Risikomanagement ohne historische Analyse unvollständig bleibt, da es keine empirische Rückkopplung zwischen Vergangenheit und Zukunft herstellt.

### 3.5 Nationaler Gefahrenkatalog

Gemäß ISO 31000 sowie ÖNORM D 4901 beginnt jede Risikoanalyse mit der Erfassung des Kontextes und der Gefahrenquellen. Der nationale Gefahrenkatalog (siehe Anhang 4) operationalisiert diesen Schritt für den österreichischen Rechtsraum. Er dient der Vereinheitlichung von Gefahrenklassen, der Sicherstellung sektorübergreifender Vergleichbarkeit und

---

<sup>86</sup> „Root Cause Analysis bedeutet Ursachenanalyse und ist eine systematische Methode zur Identifizierung der tieferliegenden Ursachen eines Problems oder unerwünschten Ereignisses, um nachhaltige Lösungen zu finden, anstatt nur Symptome zu bekämpfen und so zukünftige Vorfälle zu verhindern nach Vesely, W. E. / Goldberg, F. F. / Roberts, N. H. / Haasi, D. F. (1981).

<sup>87</sup> Aven T. (2011).

<sup>88</sup> Bundesgesetz über die Sicherstellung der staatlichen Resilienz und Koordination in Krisen (Bundes-Krisensicherheitsgesetz – B-KSG) BGBl. I Nr. 89/2023

der Priorisierung von Risiken nach Eintrittswahrscheinlichkeit und Schadensausmaß. Die Katalogstruktur des nationalen Gefahrenkataloges ordnet Gefahren in vier Gefahrenkategorien:

1. Naturgefahren (z. B. Hochwasser)
2. Technische Gefahren (z. B. Blackout)
3. Anthropogene Gefahren (z. B. soziale Unzufriedenheit)
4. Intentionale Gefahren (z. B. Sabotage)

Diese Klassifikation folgt den Grundsätzen des All-Gefahren-Ansatzes, der im RKEG ausdrücklich verankert ist und auch in der RKE-Richtlinie vorgeschrieben wird.

Der nationale Gefahrenkatalog fungiert als zentrale Datendrehscheibe und Referenz für diese Risikoanalyse ebenso wie für die betrieblichen Risikoanalysen der kritischen Einrichtungen. Jede einzelne Gefahr wird auf Grundlage einer nachvollziehbaren und extern überprüfbareren Datenbasis definiert, etwa durch wissenschaftliche Studien, Ereignisdatenbanken, Fachliteratur oder andere Ministerien. Dadurch ist gewährleistet, dass der Gefahrenkatalog methodisch valide und fachlich belastbar ist.

Der Gefahrenkatalog ist kein starres Dokument, sondern ein dynamisches Arbeitsinstrument, das unter Berücksichtigung historischer Ereignisse und verfügbarer Daten regelmäßig überarbeitet wird.

Über diese etablierten Gefahrenkategorien hinaus enthält das RKEG zwei zusätzliche Betrachtungsebenen, die bislang in keinem österreichischen Gefahrenkatalog in dieser Form abgebildet wurden und die eine wesentliche Erweiterung der bisherigen Herangehensweise darstellen. Die erste Neuerung betrifft die sektorspezifischen Abhängigkeiten innerhalb Österreichs, die von den kritischen Einrichtungen systematisch zu erfassen und bewerten sind. Dabei müssen sie nicht nur ihre eigenen Abhängigkeiten gegenüber anderen Sektoren und Teilsektoren identifizieren, etwa die Energieabhängigkeit des Gesundheitssektors oder die Wasserabhängigkeit des Lebensmittelsektors, sondern auch umgekehrt analysieren, welche Auswirkungen ein Ausfall anderer Sektoren auf die Erbringung ihres eigenen wesentlichen Dienstes hätte. Diese Betrachtung der Eintrittswahrscheinlichkeit und der Auswirkung intersektoraler Ausfälle ist neu und geht deutlich über die bislang üblichen Gefahrenklassifikationen hinaus.

Die zweite Neuerung betrifft die grenzüberschreitenden Abhängigkeiten, die das RKEG ebenfalls ausdrücklich einfordert. Kritische Einrichtungen müssen jene Dienstleistungen identifizieren, die sie im Ausland erbringen oder für die sie auf ausländische Systeme, bspw. Lieferketten, IT-Infrastrukturen oder wesentliche Komponenten angewiesen sind. Darüber hinaus ist zu analysieren, ob umgekehrt andere Staaten oder ausländische Teilsektoren in kritischem Maße von österreichischen Infrastrukturen abhängig sind. Damit rückt das RKEG globale Interdependenzen, geopolitische Abhängigkeiten und internationale Lieferketten in den Mittelpunkt der Risikoidentifikation. Aspekte, die zwar faktisch bedeutsam sind, aber in früheren österreichischen Risikoanalysen (etwa im Rahmen des APCIP) nur begrenzt oder qualitativ behandelt wurden.

Der Gefahrenkatalog mit der demonstrativen Aufzählung der Gefahren wird als strukturierter Anhang (Anhang 4) in dieser Risikoanalyse veröffentlicht und bildet das methodische Fundament aller weiteren Risikoabschätzungen im Sinne des RKEG. Durch die Kombination traditioneller Gefahrenkategorien mit den neu eingeführten internen und internationalen Abhängigkeitsdimensionen entsteht ein umfassendes, modernes und systemisches Risikobild, das den Anforderungen hochgradig vernetzter kritischer Infrastrukturen gerecht wird und eine realitätsnahe Entscheidungsgrundlage für kritische Einrichtungen ermöglicht.

# 4 Risikomanagementsystem – Organisation & Struktur

## Anforderungen gemäß ÖNORM D 4901 Normpunkte 5-7

Das Risikomanagementsystem bildet die organisatorische Grundlage für die Risikoanalyse und Risikosteuerung im Rahmen des RKEG. Die ÖNORM D 4901 definiert in den Abschnitten 5 bis 7 die strukturellen, organisatorischen und prozessualen Anforderungen an ein Risikomanagementsystem, das in bestehende Governance-Strukturen eingebettet und von der obersten Leitung getragen sein muss. Das RKEG überträgt diese Normgrundsätze auf die österreichische Verwaltungsebene und verpflichtet sowohl den Bundesminister für Inneres als auch die kritischen Einrichtungen, ein formalisiertes, dokumentiertes und überprüfbares Risikomanagementsystem einzurichten. Das Risikomanagementsystem dient dabei als Schnittstelle zwischen strategischer Steuerung (z. B. nationale Risikoanalyse, Einstufungsprozesse, Strategie) und operativer Umsetzung (z. B. betriebliche Risikoanalyse, Resilienzmaßnahmenplan). Damit erfüllt es eine zentrale Funktion in der gesamthaften Resilienzarchitektur Österreichs und stellt sicher, dass Behörden und kritische Einrichtungen nach identen Grundprinzipien und konsistenten Prozessen arbeiten.

### 4.1 Führungsaufgabe und Governance

Die ÖNORM D 4901 betont, dass Risikomanagement eine zentrale Führungsaufgabe darstellt und als integraler Bestandteil der übergeordneten Governance einer Organisation zu verstehen ist. Die oberste Leitung trägt dabei die Verantwortung, die Risikopolitik klar zu formulieren, die erforderlichen Ressourcen bereitzustellen und die organisatorischen Strukturen so auszurichten, dass Risikoanalyse und Risikosteuerung wirksam umgesetzt werden können<sup>89</sup>. Diese normative Grundhaltung wird durch das RKEG in den staatlichen Kontext übertragen. Die Bundesregierung beschließt gemäß § 9 RKEG eine nationale Strategie für die Resilienz kritischer Einrichtungen, welche die politischen Zielsetzungen, Verantwortlichkeiten und Verfahren für die Widerstandsfähigkeit kritischer Einrichtungen definiert. Damit

---

<sup>89</sup> Power, M. (2007).

übernimmt der Bundesminister für Inneres die strategische Steuerungsrolle, während die operative Verantwortung auf Seiten der kritischen Einrichtungen liegt.<sup>90</sup>

Die Erstellung dieser Risikoanalyse ist ebenfalls eine Führungsaufgabe, die dem Bundesminister für Inneres zugeordnet ist. Sie bildet das zentrale Orientierungsinstrument für sämtliche weitere Schritte im Risikomanagementprozess, etwa die Einstufung der kritischen Einrichtungen nach § 11 RKEG oder die Ableitung sektorspezifischer Schwerpunkte der Resilienzplanung. Die ÖNORM D 4901 unterstreicht, dass Führungskräfte sicherstellen müssen, dass das Risikomanagementsystem regelmäßig überprüft und an neue Rahmenbedingungen angepasst wird. Dieser Anspruch findet sich im RKEG in den wiederkehrenden Aktualisierungspflichten wieder. Risikoanalysen und Resilienzpläne müssen spätestens alle vier Jahre, oder bei veränderten Risikolagen auch früher überarbeitet werden. Dadurch entsteht ein kontinuierlicher Verbesserungsprozess, der nicht nur normativ gefordert, sondern nunmehr auch rechtlich verankert ist.

Im Zusammenspiel von Norm und Gesetz ergibt sich damit eine Governance-Struktur, die sowohl strategische Steuerung als auch operative Umsetzung umfasst. Der Bundesminister für Inneres setzt die übergeordneten Ziele, gewährleistet Kohärenz zwischen nationalen und europäischen Vorgaben und prüft die Einhaltung der Pflichten. Die kritischen Einrichtungen integrieren diese Vorgaben in ihre eigenen Organisationsstrukturen und können sich dabei auf die systematischen Anforderungen der ÖNORM D 4901, sowie auf die Richtlinien des RKEG stützen. Das Risikomanagement wird auf diese Weise zu einem gemeinsamen staatlich-privaten Steuerungssystem, das klaren Verantwortlichkeiten, transparenten Entscheidungswegen und einer regelmäßigen Wirksamkeitsprüfung folgt.<sup>91</sup>

## 4.2 Rollen und Verantwortlichkeiten

Die klare Zuordnung von Rollen und Verantwortlichkeiten bildet einen Kernbestandteil jedes wirksamen Risikomanagementsystems. Die ÖNORM Reihe D 4900 fordert ausdrücklich, dass Organisationen eindeutige Zuständigkeiten für die Planung, Umsetzung und Überwachung des Risikomanagementprozesses festlegen müssen. Damit wird sichergestellt, dass sowohl diese Risikoanalyse selbst, als auch die daraus abgeleiteten Maßnahmen nicht zufällig oder informell entstehen, sondern in einer strukturierten und nachvollziehbaren Verantwortlichkeitsarchitektur verankert sind. Dieser normative Anspruch deckt sich auch mit

---

<sup>90</sup> Renn, O. (2008).

<sup>91</sup> Aven, T. (2016).

internationalen Forschungsarbeiten, die hervorheben, dass Risikomanagement nur dann nachhaltig wirksam ist, wenn Verantwortlichkeiten klar verteilt und institutionell abgesichert sind. Mehrdeutigkeiten in Rollen und Entscheidungswegen können zu Verzögerungen, Informationsverlusten und ineffektiver Risikosteuerung führen.<sup>92</sup>

Im österreichischen System übernimmt der Bundesminister für Inneres die strategische Führungsrolle. Durch das Bundesministerium für Inneres wird diese Risikoanalyse erstellt, die Entscheidung über die Einstufung kritischer Einrichtungen getätigt und die Überwachung der Erfüllung der gesetzlichen Pflichten durchgeführt. Die operative Verantwortung liegt jedoch bei den kritischen Einrichtungen selbst, die ihre Risikoanalyse durchführen, dokumentieren und regelmäßig aktualisieren müssen. Die ÖNORM Reihe D 4900 verlangt, dass hierfür interne Rollen eindeutig festgelegt werden, typischerweise in Form von Risikomanagementbeauftragten, fachlich verantwortlichen Leitungsfunktionen oder interdisziplinären Risikoteams. Forschungsergebnisse aus dem Bereich der organisationalen Resilienz bestätigen, dass gerade klare Verantwortlichkeitsstrukturen entscheidend dafür sind, Risiken frühzeitig zu erkennen und Entscheidungen kohärent zu treffen.<sup>93</sup>

Darüber hinaus entstehen im RKEG neuartige Zuständigkeitskonstellationen, insbesondere aufgrund der Anforderungen an sektorübergreifende Abhängigkeiten, grenzüberschreitende Verflechtungen und Meldeprozesse nach §17 RKEG. Diese Elemente verlangen von kritischen Einrichtungen nicht nur ein internes Risikomanagement, sondern auch ein strukturiertes Zusammenspiel mit dem Bundesministerium für Inneres, Lieferanten und internationalen Partnern. Damit wird Risikomanagement zu einer geteilten, aber nicht diffusen Aufgabe, die intern verankert und extern abgestimmt sein muss. Insbesondere bei kritischer Infrastruktur zeigt sich, dass die Definition von Schnittstellen- und Koordinationsrollen ein wesentlicher Erfolgsfaktor für funktionierende Resilienznetzwerke ist.<sup>94</sup>

Die Verteilung von Rollen und Verantwortlichkeiten im österreichischen Resilienzsystem spiegelt somit einen governance-orientierten Ansatz wider. Die strategische Steuerung liegt beim Staat, die operative Risikoverantwortung bei den kritischen Einrichtungen, während die ÖNORM Reihe D 4900 als methodischer Rahmen sicherstellt, dass diese Rollen in den Organisationen nicht nur benannt, sondern funktional verankert sind. Dadurch entsteht

---

<sup>92</sup> Jerab, D. A. (2023).

<sup>93</sup> Duchek, S. (2020).

<sup>94</sup> Kuipers, S. / Wolbers, J. (2021).

eine klare Aufgabenarchitektur, die Transparenz schafft, Verantwortlichkeiten absichert und eine konsistente Umsetzung des RKEG gewährleistet.

### 4.3 Integration in nationale Strategien und Systeme

Risikomanagement kann seine Funktionen nur dann wirksam erfüllen, wenn es eng mit bestehenden strategischen und administrativen Steuerungsmechanismen verknüpft ist. In Österreich ist diese Einbettung entscheidend, da das RKEG ein mehrstufiges System schafft, in dem staatliche Führung, sektorspezifische Vorgaben und betriebliche Risikoanalysen aufeinander abgestimmt sein müssen. Erst durch diese Verknüpfung entsteht ein konsistentes Resilienzsystem, das nationale Ziele, europäische Anforderungen und betriebliche Prozesse miteinander verbindet. Die ÖNORM D 4901 bietet hierfür den methodischen Bezugsrahmen, indem sie beschreibt, wie Risikomanagement in bestehende Strategie- und Planungssysteme integriert werden soll, ohne selbst staatliche Vorgaben zu setzen.

Der übergeordnete nationale Rahmen wird durch die Österreichische Sicherheitsstrategie 2024<sup>95</sup>, die Österreichische Cybersicherheitsstrategie 2021<sup>96</sup>, die Österreichische Strategie zur Anpassung an den Klimawandel<sup>97</sup> sowie durch die operative Koordination des Staatlichen Krisen- und Katastrophenmanagements (SKKM)<sup>98</sup> geprägt. Seit 2026 wird dieser strategische Rahmen durch die Österreichische Strategie für die Resilienz Kritischer Einrichtungen ergänzt, die erstmals eine einheitliche nationale Linie für den Schutz kritischer Einrichtungen formuliert. Diese Strategie operationalisiert die Anforderungen des RKEG und der RKE-Richtlinie und legt Grundprinzipien, Verantwortlichkeiten und langfristige Zielsetzungen für Behörden und kritische Einrichtungen fest. Damit fungiert sie als verbindendes Element zwischen staatlichen Zielsetzungen, sektorspezifischen Vorgaben und den betrieblichen Risikoanalysen der kritischen Einrichtungen. Forschungsergebnisse zur staatlichen Resilienzpolitik zeigen, dass derartige nationale Strategiedokumente eine zentrale Funktion übernehmen, indem sie Koordination erleichtern, Bewertungsmaßstäbe vereinheitlichen und sektorübergreifende Prioritäten sichtbar machen.<sup>99</sup>

---

<sup>95</sup> BKA (2024).

<sup>96</sup> BKA (2021).

<sup>97</sup> BMKUMIT (2024).

<sup>98</sup> BMI (2024a).

<sup>99</sup> Christensen, T. / Læg Reid, P. / Rykkja, L. H. (2016).

Im Rahmen des RKEG wird diese Integration durch drei zentrale Mechanismen operationalisiert. Erstens wird diese Risikoanalyse als Referenzrahmen für die Risikoanalysen der kritischen Einrichtungen definiert, sodass eine gemeinsame Daten- und Bewertungskonfiguration entsteht. Zweitens verpflichtet das RKEG die kritischen Einrichtungen, ihre Ergebnisse in strukturierter Form vorzulegen, was eine unmittelbare Vergleichbarkeit und Weiterverarbeitung im staatlichen System ermöglicht. Drittens werden die Resilienzpläne und Meldepflichten so gestaltet, dass sie sowohl sektorinterne Anforderungen als auch nationale und europäische Vorgaben berücksichtigen. Damit orientiert sich das österreichische System an internationalen Erkenntnissen, wonach Resilienz nur dann entsteht, wenn staatliche und private Akteure ihre Risikobewertungen aufeinander abstimmen und gemeinsame Prioritäten entwickeln.<sup>100</sup>

Die Integration des Risikomanagements in nationale Strategien ist jedoch nicht nur funktionale Abstimmung, sondern auch ein Governance-Instrument. Durch gemeinsame Kriterien, abgestimmte Risikodefinitionen, regelmäßige Datenflüsse und strukturierte Kommunikationswege wird vermieden, dass kritische Einrichtungen und verschiedene Bundesministerien getrennte Risikowelten erzeugen. Stattdessen entsteht ein kohärentes, mehrstufiges System, in dem betriebliche Risikoanalysen Teil einer übergeordneten staatlichen Resilienzarchitektur sind. Die ÖNORM Reihe D 4900 liefert hierfür den methodischen Rahmen, das RKEG den verbindlichen rechtlichen Auftrag und die nationalen Strategiedokumente die politischen Leitlinien. So entsteht ein Risikomanagementsystem, das sowohl organisationsintern konsistent als auch national integriert wirkt und damit jene Voraussetzung schafft, die Forschung und internationale Standards als entscheidenden Erfolgsfaktor resilienter Infrastrukturen hervorheben.

---

<sup>100</sup> Alexander, D. (2016).

# 5 Risikomanagementprozess

## Anforderungen gemäß ÖNORM D 4901 Normpunkt 8

Der Risikomanagementprozess bildet das operative Zentrum jeder Risikoanalyse und stellt sicher, dass Risiken systematisch, nachvollziehbar und konsistent behandelt werden. Gemäß der ÖNORM D 4901 umfasst dieser Prozess eine Reihe klar strukturierter Schritte, die in ihrer Gesamtheit einen zirkulären und lernorientierten Ablauf ergeben. Ziel ist es, Risiken nicht nur zu identifizieren und zu bewerten, sondern sie in einen kontinuierlichen Entscheidungs- und Steuerungsprozess einzubetten, der auf Rückkopplung, Transparenz und laufender Verbesserung basiert.

Im österreichischen Kontext ist dieser Prozess unmittelbar mit den Anforderungen des RKEG verbunden, das einen vergleichbaren und überprüfbaren Umgang mit Risiken kritischer Einrichtungen sicherstellen soll. Die Struktur des Prozesses ermöglicht es, komplexe Risikolagen methodisch zu erfassen, Abhängigkeiten sichtbar zu machen und Maßnahmen zielgerichtet abzuleiten. Gleichzeitig gewährleistet der prozessorientierte Aufbau, dass Risikoanalysen regelmäßig aktualisiert und an neue Rahmenbedingungen angepasst werden können.

Die folgenden Unterkapitel orientieren sich an der prozessualen Logik der ÖNORM D 4901 und beschreiben detailliert die einzelnen Schritte des Risikomanagementprozesses, von der Kommunikation und Konsultation über die Identifikation und Analyse bis hin zur Bewertung, Behandlung sowie der kontinuierlichen Überwachung und Überprüfung. Damit wird ein kohärentes und nachvollziehbares Prozessmodell dargestellt, das sowohl den methodischen Anforderungen der Norm als auch den gesetzlichen Vorgaben des RKEG entspricht.

### 5.1 Prozessübersicht

Ein wirkungsvolles Risikomanagement beruht auf einem klar strukturierten, wiederkehrenden Prozess, der Risiken nicht nur identifiziert und bewertet, sondern auch in Entscheidungen, Maßnahmen und organisatorisches Lernen überführt. Die ISO 31000 beschreibt diesen Prozess als zirkulären Managementablauf, dessen Schritte in einem kontinuierlichen Ver-

besserungszyklus miteinander verflochten sind. Wissenschaftliche Analysen der Norm betonen, dass diese Struktur nicht als starre Abfolge, sondern als dynamisches System wechselseitiger Rückkopplungen zu verstehen ist, das Organisationen befähigt, auf Unsicherheiten adaptiv zu reagieren.<sup>101</sup> Die ÖNORM D 4901 setzt diesen Ansatz für den österreichischen Anwendungsraum um, indem sie die Prozessschritte präzise operationalisiert und Anforderungen an deren formale Dokumentation formuliert.

Für kritische Einrichtungen gewinnt diese Prozesslogik besondere Bedeutung, da das RKEG einen vergleichbaren und transparenten Umgang mit Risiken vorschreibt. Diese Risikoanalyse bildet den übergeordneten Bezugsrahmen, der sicherstellt, dass alle kritische Einrichtungen nach einem einheitlichen Verständnis von Risikoarten, Abhängigkeiten und Bewertungskriterien arbeiten. Der Risikomanagementprozess dient daher nicht nur dem betrieblichen Schutz, sondern ist gleichzeitig Teil einer staatlich koordinierten Resilienzarchitektur. Diese doppelte Funktion, operativ wirksam und institutionell anschlussfähig zu sein, macht es erforderlich, dass der Prozess klar strukturiert, nachvollziehbar dokumentiert und fortlaufend gepflegt wird.

Ein zentrales Merkmal dieses Prozesses liegt in seinem iterativen Charakter. Risiken ändern sich, Abhängigkeiten entwickeln sich weiter und neue Bedrohungen entstehen, sei es durch technologische Innovation, soziale Dynamiken oder geopolitische Veränderungen. Genau diese Perspektive spiegelt sich im RKEG wider, das regelmäßige Aktualisierungen der Risikoanalyse sowie eine fortlaufende Überprüfung der Resilienzpläne verlangt.

Die Prozessübersicht verdeutlicht somit, dass Risikomanagement in kritischen Einrichtungen kein einmaliger Auftrag, sondern ein dauerhaft angelegter organisatorischer Kernprozess ist. Er verbindet normative Anforderungen, wie sie in der ÖNORM D 4901 formuliert sind, mit den rechtlichen Vorgaben des RKEG und schafft die methodische Grundlage für ein einheitliches, vergleichbares und transparentes Risikoverständnis im gesamten österreichischen Resilienzsystem.

---

<sup>101</sup> Luko, S. N. (2013).

## 5.2 Kommunikation und Konsultation

Kommunikation und Konsultation bilden den durchgängigen Rahmen des gesamten Risikomanagementprozesses. Sie gewährleisten, dass Risikoinformationen nicht isoliert entstehen, sondern im Austausch zwischen unterschiedlichen Fachbereichen, Entscheidungsebenen und externen Partnern bewertet werden. In der ISO 31000 wird dieser kontinuierliche Dialog als zentrale Voraussetzung dafür beschrieben, Risiken nachvollziehbar und gemeinsam getragen zu beurteilen.<sup>102</sup> Die ÖNORM D 4901 überträgt dieses Prinzip auf den österreichischen Kontext, indem sie fordert, Risikomanagement als dialogorientierten und interdisziplinären Prozess zu gestalten.

Für kritische Einrichtungen ist Kommunikation besonders bedeutsam, weil das RKEG komplexe Informations- und Abstimmungsprozesse zwischen ihnen, dem Bundesminister für Inneres und relevanten Stakeholdern vorsieht. Konsultationsverfahren ermöglichen es, technische, organisatorische und sicherheitsrelevante Perspektiven zusammenzuführen, etwa bei der Bewertung sektorübergreifender Abhängigkeiten oder grenzüberschreitender Risiken.

Darüber hinaus erhöhen strukturierte Kommunikations- und Konsultationsmechanismen die Robustheit des gesamten Resilienzsystems. Sie reduzieren Informationsbrüche, verbessern die Abstimmung zwischen einzelnen Akteuren und stärken die institutionelle Einbindung der betrieblichen Risikoanalyse in staatliche Steuerungsstrukturen. Effektive Risikokommunikation schafft damit nicht nur Transparenz, sondern fördert auch Vertrauen und Koordinationsfähigkeit, zwei Aspekte, die für kritische Einrichtungen essenziell sind.<sup>103</sup>

Ein zentrales Element dieser Konsultationsprozesse waren durchgeführte Workshops mit den maßgeblichen Akteuren ausgewählter Sektoren also jenen Unternehmen bzw. Organisationen, die mit hoher Wahrscheinlichkeit in den Anwendungsbereich des RKEG fallen. Diese Workshops dienen der gemeinsamen Entwicklung eines konsistenten Risikoverständnisses innerhalb des Sektors. Im Rahmen dieser Treffen wurden insbesondere die Skalierung der Eintrittswahrscheinlichkeit und des Auswirkungsgrades aus Sicht des Bundesministers für Inneres vorgestellt, der nationale Gefahrenkatalog inklusive der Gefahrenkategorien und Gefahrenbeschreibungen erläutert sowie alle Gefahren des Katalogs gemeinsam bewertet. Darüber hinaus identifizierten und bewerteten die Teilnehmerinnen und Teilneh-

---

<sup>102</sup> Purdy, G. (2010).

<sup>103</sup> Lundgren, R. E. / McMakin, A. H. (2018).

mer sektorspezifische Gefahren sowie Risiken mit sektorübergreifenden und grenzüberschreitenden Auswirkungen. Damit trugen die Workshops wesentlich dazu bei, fachliche Expertise mit staatlichen Bewertungsmaßstäben zu verknüpfen und ein harmonisiertes Risikobild innerhalb des jeweiligen Sektors, welches für die Risikoanalyse auf sektoraler Ebene notwendig ist, zu entwickeln.

### 5.3 Rahmenbedingung und Risikokriterien

Eine präzise Definition der Rahmenbedingungen und Gefahrenkategorien bildet die Grundlage jeder Risikoanalyse. Dieser Schritt legt fest, welche Ziele verfolgt werden, welche Annahmen gelten, welche Grenzen bestehen und wonach im weiteren Sinn Risiken bewertet werden. Die ISO 31000 beschreibt diesen Prozess als essenziell, um sicherzustellen, dass Risikoanalysen konsistent, vergleichbar und in den organisatorischen Kontext eingebettet sind.<sup>104</sup> Die ÖNORM D 4901 überträgt diesen Ansatz auf den österreichischen Raum, indem sie klare Anforderungen an die Festlegung von Bewertungsmaßstäben, Verantwortlichkeiten und Risikoakzeptanzgrenzen formuliert.

Im RKEG-Kontext ist die Festlegung der Rahmenbedingungen besonders anspruchsvoll, weil Risikoanalysen kritischer Einrichtungen nicht nur interne Faktoren berücksichtigen müssen, sondern auch staatliche Vorgaben, intersektorale Abhängigkeiten, grenzüberschreitende Auswirkungen und die Ergebnisse dieser Risikoanalyse. Dadurch entsteht ein mehrschichtiger Bewertungsrahmen, der sowohl betriebliche Perspektiven als auch nationale Prioritäten einbindet. Risikokriterien, wie Eintrittswahrscheinlichkeit und Auswirkung müssen daher so definiert werden, dass sie nachvollziehbar und überprüfbar sind.

Die nachstehenden Skalen wurden so gestaltet, dass sie den unterschiedlichen Charakteristika der jeweiligen Gefahrenkategorien entsprechen. Naturgefahren lassen sich typischerweise anhand historischer Ereignisdaten quantifizieren, während intentionale Gefahren stärker durch die Handlungen von Akteuren geprägt sind und daher andere zeitliche Bewertungsintervalle erfordern. Anthropogene und technische Gefahren wiederum werden häufig durch Plausibilitätsüberlegungen und Erfahrungen im Betriebskontext bewertet. Zusätzlich berücksichtigt das österreichische Resilienzsystem im Sinne des RKEG zwei besondere

---

<sup>104</sup> Purdy, G. (2010).

Dimensionen, sektorenübergreifende Abhängigkeiten und Auswirkungen auf die Verfügbarkeit wesentlicher Dienste, wie sie in der Delegierten Verordnung (EU) 2023/2450 definiert sind.

Die im Anhang 2 ersichtlichen Skalen definieren daher sowohl die Eintrittswahrscheinlichkeit (EW) für alle geforderten Gefahrenkategorien als auch das Schadensausmaß (A) im Hinblick auf die Verfügbarkeit des wesentlichen Dienstes. Zusammen bilden sie die belastbare Bewertungsgrundlage für die nationale Risikoanalyse und ermöglichen sowohl eine qualitative als auch eine semi-quantitative Bewertung<sup>105</sup>. Die semi-quantitative Methode kommt zur Anwendung, wenn eine Ermittlung von Eintrittswahrscheinlichkeiten und Auswirkungen für ein Szenario aufgrund teilweise fehlender Datengrundlagen nicht gänzlich quantitativ möglich ist; es kann beispielsweise für ein bestimmtes Szenario das zu erwartende Schadensausmaß gut beschrieben sein, für die Eintrittswahrscheinlichkeit jedoch keine genauen Daten zur Verfügung stehen. In solchen Fällen müssen die fehlenden Daten durch Abschätzungen ergänzt werden. Die Skalen sind so aufgebaut, dass sie unmittelbar in die Risikomatrix, welche im Kapitel 6.7 erläutert wird, überführt werden können.

Durch diese strukturierte und differenzierte Skalierung wird gewährleistet, dass die nationale Risikoanalyse nicht nur methodisch korrekt durchgeführt werden kann, sondern auch die besonderen Anforderungen des RKEG erfüllt. Klar formulierte Risikokriterien sind ein entscheidender Erfolgsfaktor, da sie Transparenz schaffen, Unsicherheiten reduzieren und eine systematische Bewertung ermöglichen.

## 5.4 Risikoidentifikation

Die Risikoidentifikation bildet den ersten operativen Schritt der nationalen Risikoanalyse und verfolgt das Ziel, alle potenziellen Gefahren, Bedrohungen und relevanten Einflussfaktoren systematisch zu erfassen. Die ISO 31000 sowie die ÖNORM D 4901 betonen, dass Risikoidentifikation nicht als rein technischer Vorgang zu verstehen ist, sondern als strukturierter Prozess, der unterschiedliche Wissensquellen zusammenführt. Für diese Risikoanalyse bedeutet dies, dass die Identifikation nicht nur auf historischen Daten und wissen-

---

<sup>105</sup> BMI (2018).

schaftlichen Erkenntnissen aufgebaut wurde, sondern auch auf sektoralen Erfahrungswerten, Fachwissen aus den Ressorts, nationalen und europäischen Lagebildern sowie Ergebnisberichten aus bestehenden Krisen- und Sicherheitsstrukturen basieren.

Gemäß RKEG ist diese Risikoanalyse darauf ausgerichtet, ein übergreifendes Risikobild für Österreich zu schaffen, das alle kritischen Einrichtungen und ihre Abhängigkeiten berücksichtigt. Grundlage hierfür bildet der nationale Gefahrenkatalog, der als systematische Struktur dient, um Gefahren in definierte Kategorien zu ordnen und deren Relevanz für das Gesamtsystem zu beschreiben. Die Risikoidentifikation umfasst daher sowohl die Prüfung und Aktualisierung dieses Gefahrenkatalogs als auch die Einbeziehung neuer oder veränderter Risikolagen, die sich aus technologischen Entwicklungen, internationalen Abhängigkeiten oder geänderten Bedrohungsszenarien ergeben können.

Ein wesentlicher Bestandteil der Risikoidentifikation innerhalb der nationalen Risikoanalyse sind die sektoralen Workshops und Konsultationen mit den voraussichtlich betroffenen kritischen Einrichtungen. Diese Austauschformate dienen dazu, sektorspezifische Gefahren, sektorübergreifende Abhängigkeiten und grenzüberschreitende Auswirkungen einzubeziehen, die in rein analytischen Modellen häufig nur unzureichend abgebildet werden können. Der nationale Gefahrenkatalog wird durch diese Rückmeldungen ergänzt, wodurch eine gemeinsame, sektorübergreifende Grundlage entsteht.

Die Risikoidentifikation im Rahmen dieser Risikoanalyse verfolgt somit einen mehrstufigen Ansatz, wissenschaftlich fundiert, normgemäß strukturiert, durch sektorale Expertise ergänzt und eingebettet in die gesetzlichen Vorgaben des RKEG.

## **5.5 Risikoanalyse**

Der nächste Analyseschritt im Rahmen dieser nationalen Risikoanalyse ist wortident und hat den Zweck, die zuvor identifizierten Gefahren systematisch hinsichtlich ihrer Eintrittswahrscheinlichkeit und ihrer potenziellen Auswirkungen auf Österreichs kritische Einrichtungen zu bewerten. Die ISO 31000 und die ÖNORM D 4901 definieren Risikoanalyse als einen methodisch fundierten Prozess, der Unsicherheiten sichtbar macht, Zusammenhänge verständlich aufbereitet und die Grundlage für eine spätere Priorisierung schafft. Für die nationale Ebene bedeutet dies, Risiken nicht isoliert zu betrachten, sondern sie im Kontext der staatlichen Gesamtverantwortung und sektorübergreifenden Interdependenzen zu bewerten.

Der Analyseschritt stützt sich auf eine harmonisierte Bewertungslogik, die in Österreich durch die im RKEG verankerten Anforderungen sowie durch die entwickelten Skalen operationalisiert wird. Die Eintrittswahrscheinlichkeit wird differenziert nach Gefahrenkategorien bewertet, um der spezifischen Natur von technischen Gefahren, anthropogenen Gefahren, intentionalen Gefahren und Naturgefahren, sowie sektorenübergreifenden Abhängigkeiten gerecht zu werden. Parallel dazu erfolgt die Bewertung der Auswirkungen auf Basis der Verfügbarkeit der wesentlichen Dienste gemäß Delegierter Verordnung (EU) 2023/2450. Dadurch wird sichergestellt, dass Risiken einheitlich, nachvollziehbar und über alle Sektoren hinweg vergleichbar erfasst werden.

Diese Risikoanalyse gewinnt durch die Zusammenführung von qualitativen und quantitativen Informationen an Aussagekraft.<sup>106</sup> Die Kombination unterschiedlicher Wissensarten, bspw. statistischer Daten, Szenarioanalysen, Experteneinschätzungen und empirischer Erfahrungswerte tragen dazu bei, Unsicherheiten zu reduzieren und ein realistischeres Risikobild zu erzeugen. Für diese Risikoanalyse ist daher ein multimethodischer Ansatz erforderlich, der sowohl historische Ereignisdaten als auch sektorale Expertise und institutionelle Lagebilder integriert. Im Rahmen dieser Risikoanalyse wurde dieser Ansatz so operationalisiert, dass die Bewertung zunächst auf Ebene der Teilsektoren erfolgte, insbesondere in den differenzierten Sektoren Verkehr und Energie. Die daraus resultierenden Bewertungen wurden im nächsten Schritt zu sektoralen Risikoübersichten aggregiert und anschließend zu einem gesamtstaatlichen Risikobild synthetisiert. Dadurch entsteht eine vertikal integrierte Risikostruktur, die sowohl die Besonderheiten einzelner Teilsektoren als auch deren Beitrag zur nationalen Gesamtrisikolage abbildet.

Eine Besonderheit der Risikoanalyse im Kontext des RKEG liegt in der verstärkten Berücksichtigung systemischer Risiken. Österreichs kritische Sektoren sind eng miteinander vernetzt, sodass Störungen in einem Bereich erhebliche Folgeeffekte in anderen Sektoren auslösen können. Die Analyse dieser Interdependenzen, insbesondere die Bewertung sektorübergreifender Abhängigkeiten, ist ein zentrales Element des Risikomanagements auf nationaler Ebene. Die Struktur der ISO 31000 unterstützt diesen systemischen Blick, da sie explizit die Notwendigkeit hervorhebt, Wechselwirkungen, Kontextfaktoren und Unsicherheiten strukturiert zu berücksichtigen.

---

<sup>106</sup> Aven, T. / Zio, E. (2017).

Insgesamt stellt die Risikoanalyse einen analytischen Kernprozess dar, der die Komplexität nationaler Risikolandschaften erfassbar macht und die Entscheidungsgrundlage für die nachfolgende Risikobewertung und die Festlegung nationaler Prioritäten bildet.

## 5.6 Risikobewertung

Die Risikobewertung bildet die Schnittstelle zwischen der analytischen Erfassung von Risiken und der staatlichen Priorisierung. Während die Analyse die Eintrittswahrscheinlichkeit und das Ausmaß möglicher Auswirkungen ermittelt, bezweckt die Risikobewertung, diese Ergebnisse im Hinblick auf ihre strategische und gesamtstaatliche Bedeutung einzuordnen. Die ISO 31000 und die ÖNORM D 4901 beschreiben diesen Schritt als Entscheidungsprozess, der Bewertungskriterien, Risikotoleranzen und übergeordnete Ziele berücksichtigt, um zu bestimmen, welche Risiken besondere Aufmerksamkeit erfordern und welche nachrangig behandelt werden können.

Im Rahmen dieser Risikoanalyse erfolgt die Risikobewertung auf Grundlage einheitlicher Kriterien. Hierzu zählen insbesondere:

- die harmonisierte Skalierung der Eintrittswahrscheinlichkeit und des Schadensausmaßes,
- die sektorale Relevanz,
- die Kritikalität für die Aufrechterhaltung wesentlicher Dienste,
- die Stärke sektorübergreifender Abhängigkeiten,
- das potenzielle Ausbreitungs- und Kaskadenpotenzial,
- die Relevanz für europäische und internationale Verpflichtungen.

Diese Kriterien ermöglichen es, Risiken nicht nur anhand isolierter Werte zu beurteilen, sondern ihre systemische Bedeutung für das österreichische Resilienzsystem zu bewerten. Die Bewertung erfolgt in mehreren Stufen: Zunächst werden die Risiken innerhalb der jeweiligen Teilsektoren gereiht, anschließend auf Sektorebene konsolidiert und schließlich in eine gesamtstaatliche Reihung überführt. Diese Aggregationslogik gewährleistet, dass sektorale Besonderheiten berücksichtigt werden, gleichzeitig aber ein übergreifendes Lagebild entsteht, das für die staatliche Steuerung zentral ist.

Die Risikobewertung bildet somit den entscheidenden Schritt, um die Vielzahl potenzieller Risiken in eine geordnete Struktur zu überführen und daraus nationale Prioritäten abzuleiten. Sie stellt sicher, dass Ressourcen, politische Aufmerksamkeit und planerische Maßnahmen dort eingesetzt werden, wo sie den größten Beitrag zur Resilienz Österreichs leisten können.

## 5.7 Risikobehandlung

Die Risikobehandlung bildet den abschließenden Schritt der nationalen Risikoanalyse und schafft die Grundlage für staatliche Maßnahmen zur Erhöhung der Resilienz kritischer Einrichtungen. Während die Risikobewertung bestimmt, welche Risiken vorrangig adressiert werden müssen, beschreibt die Risikobehandlung jene strategischen Optionen, mit denen diese Risiken reduziert, kontrolliert oder anders bewältigt werden können. Die ISO 31000 und die ÖNORM D 4901 definieren hierzu vier Grundstrategien:

- Risikovermeidung,
- Risikoverminderung,
- Risikoübertragung,
- Risikoakzeptanz.

Im Kontext des § 10 RKEG bedeutet Risikobehandlung nicht die direkte Umsetzung operativer Maßnahmen, sondern die Ableitung staatlicher Handlungsschwerpunkte. Dazu gehören etwa Empfehlungen zur Anpassung regulatorischer Rahmenbedingungen, die Identifikation von Bereichen mit besonderem Handlungsbedarf oder die Entwicklung von Maßnahmen. Die Risikobehandlung dient somit als Brücke zwischen analytischem Prozess und politisch-strategischer Steuerung, welche zur Stärkung der gesamtstaatlichen Resilienz erforderlich ist.

## 5.8 Überwachung und Review

Die Überwachung und Überprüfung stellt sicher, dass die nationale Risikoanalyse ein dynamisches und aktuelles Steuerungsinstrument bleibt. Risiken verändern sich durch neue Bedrohungen, technische Entwicklungen, internationale Abhängigkeiten oder organisatorische Veränderungen. Deshalb betonen ISO 31000 und die ÖNORM Reihe D 4900, dass Risi-

komanagementprozesse zyklisch aufgebaut sein müssen: Ergebnisse werden nicht nur dokumentiert, sondern regelmäßig hinterfragt, aktualisiert und verbessert. Dieser zyklische Charakter kann als einer der zentralen konzeptionellen Pfeiler der ISO 31000 angesehen werden, da nur durch fortlaufendes Monitoring ein belastbares Risikobild aufrechterhalten werden kann.<sup>107</sup>

Für diese Risikoanalyse bedeutet dies, dass kontinuierlich sicherheitsrelevante Informationen gesammelt und analysiert werden müssen. Dazu gehören Entwicklungen in den Sektoren, Erkenntnisse aus sicherheitsrelevanten Vorfällen, internationale Lagebilder sowie technische und organisatorische Veränderungen. Auch Rückmeldungen aus den sektoralen Workshops, Änderungen im Gefahrenkatalog oder die Ergebnisse der Risikoanalysen der kritischen Einrichtungen fließen in die laufende Überprüfung ein. Die ÖNORM D 4901 verweist explizit darauf, dass Monitoring nicht nur den Risikooutput, sondern auch die verwendeten Methoden, Kriterien und Entscheidungsgrundlagen umfasst.

Die Überprüfung erfolgt in festgelegten Intervallen oder bei wesentlichen Veränderungen der Risikolandschaft. Dabei werden Risikokriterien, Bewertungslogiken, Skalierungen und sektorübergreifende Abhängigkeiten neu bewertet. Im Kontext der ISO 31000 ist dieser Prozessschritt entscheidend für die Qualitätssicherung, da er sicherstellt, dass sich der Risikomanagementprozess an neue Informationen anpasst und die Organisation lernfähig bleibt.<sup>108</sup>

Insgesamt gewährleistet die Überwachung und Überprüfung, dass die nationale Risikoanalyse ein zuverlässiges, aktuelles und lernfähiges Lageinstrument bleibt. Sie unterstützt die kontinuierliche Weiterentwicklung des staatlichen Resilienzsystems und stellt sicher, dass politische Entscheidungen auf aktuellen und überprüften Risikodaten basieren.

---

<sup>107</sup> Leitch, M. (2010).

<sup>108</sup> Edwards, P. / Bowen, P. (2004).

# 6 Risikobewertung & Ergebnisse

## Anforderungen gemäß ÖNORM D 4901 Normpunkt 9

Dieses Kapitel präsentiert die zentralen Ergebnisse dieser Risikoanalyse und fasst jene Risiken zusammen, die für Österreichs gesamtstaatliche Sicht für kritische Einrichtungen von besonderer Relevanz sind. Die Bewertung erfolgt auf Grundlage der in Kapitel 5 beschriebenen Methoden, Skalen und Kriterien und orientiert sich an den Anforderungen der ÖNORM D 4901, die eine transparente und nachvollziehbare Darstellung der Resultate vorsieht.

Da diese Risikoanalyse im Zeitpunkt der Erstellung auf einem mehrstufigen, noch laufenden Konsultationsprozess basiert, konnten für einige Sektoren bislang keine vollständigen Daten erhoben werden. Dies betrifft insbesondere jene Bereiche, in denen Workshops mit potenziell kritischen Einrichtungen noch ausstehen oder in denen die Identifikation der betroffenen kritischen Einrichtungen gemäß RKEG noch nicht abgeschlossen ist. Erst nach Abschluss dieser sektoralen Erhebungen und der finalen Bestimmung der kritischen Einrichtungen können die Datenlücken geschlossen und die Risikoanalyse vollständig validiert werden.

Die in diesem Kapitel dargestellten Ergebnisse sind daher als vorläufige, aber fachlich belastbare Zwischenstände zu verstehen, die auf der besten verfügbaren Datenlage basieren. Sie ermöglichen bereits jetzt eine erste Priorisierung der Risiken für die gesamtstaatliche Resilienzplanung.

Zur besseren Übersicht werden die zentralen Risikokategorien zunächst in Form einer gesamtstaatlichen Ergebnisübersicht zusammengefasst. Im Anschluss folgen detaillierte Darstellungen nach Teilsektoren, sektorübergreifenden Auswirkungen, grenzüberschreitenden Risiken, klimawandelbedingten Gefahren, Low-Probability/High-Impact-Risiken sowie Emerging Risks. Diese Struktur ermöglicht eine eindeutige Zuordnung der Risiken und zeigt zugleich die Interdependenzen zwischen den Sektoren auf.

Die im Folgenden dargestellten relevanten Risiken bieten damit eine erste konsolidierte Risikoperspektive aus staatlicher Sicht. Sie bilden den Ausgangspunkt für die fortlaufende Aktualisierung dieser Risikoanalyse.

- Pandemie/Epidemie
- Hochwasser
- Dürre
- Sonstige geologische Extremereignisse (u.a. rückführbar auf Klimawandel)
- Sonstige klimatische bzw. meteorologische Extremereignisse (u.a. rückführbar auf Klimawandel)
- Abhängigkeiten von ausländischen Technologien
- Fehlendes Fachpersonal
- Blackout
- Internet Blackout
- Sabotage
- Spionage und nachrichtendienstliche Aktivitäten
- Ideologisch oder religiös motivierte Gewalthandlungen
- Staatlich, ideologisch oder religiös motivierte Handlungen
- Störung in der Strominfrastruktur
- Cyberkriminalität im engeren Sinn
- Cyberspionage
- Cybersabotage
- Cyber-Attacke auf kritische IKT-Systeme die physisch mit Stromnetzversorgungsnetzen verbunden sind (Übertragungs-/Verteilernetze, Kraftwerke, Industriebetriebe)
- Fehlerhafte Software
- Unsichere Hardware
- Technisches Gebrechen
- Drohnenangriff

## 6.1 Risiken nach Sektoren und Teilsektoren

Die Bewertung der Risiken auf Ebene der Sektoren und Teilsektoren bildet einen zentralen Bestandteil dieser Risikoanalyse. Aufgrund der engen funktionalen und technischen Verflechtungen innerhalb einzelner Bereiche, insbesondere in den Sektoren Energie, Verkehr, Gesundheit, digitale Infrastruktur und öffentliche Verwaltung ist eine sektorale Differenzierung erforderlich, um die spezifischen Gefährdungslagen präzise erfassen zu können.

Bei den nachfolgend aufgelisteten Gefahren handelt es sich um relevante und spezifische Risiken für die jeweiligen Sektoren bzw. Teilsektoren. Dies bedeutet jedoch nicht, dass andere Gefahren aus dem Gefahrenkatalog nicht zutreffend sind, sondern müssen durch jede

kritische Einrichtung einzeln bewertet werden. Diese relevante und sektorspezifische Risiken dienen als strukturelle Grundlage der Risikoanalyse und sollten auf jeden Fall durch kritische Einrichtungen betrachtet werden. Im weiteren Verlauf des RKEG-Umsetzungsprozesses werden diese Risiken hinsichtlich Eintrittswahrscheinlichkeit und Auswirkung kontinuierlich evaluiert und neu bewertet. Eine Veröffentlichung erfolgt spätestens alle vier Jahre, anlassbezogen früher.

### **Sektor Energie - Teilsektor Strom:**

- Hochwasser
- Sturm
- Sonstige geologische Extremereignisse (u.a. rückführbar auf Klimawandel)
- Sonstige klimatische bzw. meteorologische Extremereignisse (u.a. rückführbar auf Klimawandel)
- Abhängigkeiten von ausländischen Technologieanbietern und deren Dienstleistungen
- Rohstoffmangel
- Gasmangellage
- Internet Blackout
- Spionage und nachrichtendienstliche Aktivitäten
- Kaskadeneffekt
- Ideologisch oder religiös motivierte Gewalthandlungen
- Staatlich, ideologisch oder religiös motivierte Handlungen
- Störung der Gasinfrastruktur
- Störung in der Strominfrastruktur
- Anschlag mit elektromagnetischer Waffe
- Cyberkriminalität im engeren Sinn
- Cyberspionage
- Cybersabotage
- Cyber-Attacke auf kritische IKT-Systeme die physisch mit Stromnetzversorgungsnetzen verbunden sind (Übertragungs-/Verteilernetze, Kraftwerke, Industriebetriebe)
- Fehlerhafte Software
- Unsichere Hardware
- Drohnenangriff
- Ausfall der Informations- und Kommunikationssysteme für Echtzeitanwendungen
- Blackout
- Simultaner Ausfall von Hoch- / Höchstspannungskomponenten im Elektrizitätssystem

### **Sektor Energie - Teilsektor Fernwärme & -kälte:**

- Rohstoffmangel
- Gasmangellage
- Internet Blackout
- Spionage und nachrichtendienstliche Aktivitäten
- Störung der Gasinfrastruktur
- Störung in der Strominfrastruktur
- Cyberkriminalität im engeren Sinn
- Cyberspionage
- Cybersabotage
- Fehlerhafte Software
- Unsichere Hardware
- Drohnenangriff
- Blackout

### **Sektor Energie - Teilsektor Erdöl:**

- Hochwasser
- Sonstige klimatische bzw. meteorologische Extremereignisse (u.a. rückführbar auf Klimawandel)
- Sonstige geologische Extremereignisse (u.a. rückführbar auf Klimawandel)
- Mangelndes Sicherheitsbewusstsein
- Rohstoffmangel
- Internet Blackout
- Spionage und nachrichtendienstliche Aktivitäten
- Sanktionen und wirtschaftliche Zwangsmaßnahmen
- Störung in der Ölinfrastruktur
- Drohnenangriff
- Cyberkriminalität im engeren Sinn
- Cyberspionage
- Cybersabotage
- Cyber-Attacke auf kritische IKT-Systeme die physisch mit Stromnetzversorgungsnetzen verbunden sind (Übertragungs-/Verteilernetze, Kraftwerke, Industriebetriebe)
- Fehlerhafte Software
- Schwerer Industrieunfall mit gefährlichen Stoffen
- Ausfall der Informations- und Kommunikationssysteme für Echtzeitanwendungen

- Technisches Gebrechen
- NATECH<sup>109</sup>

### **Sektor Energie - Teilsektor Erdgas:**

- Sonstige geologische Extremereignisse (u.a. rückführbar auf Klimawandel)
- Abhängigkeiten von ausländischen Technologieanbietern und deren Dienstleistungen
- Rohstoffmangel
- Gasmangellage
- Störung weltraumbezogener Infrastruktur
- Innentäterschaft
- Internet Blackout
- Spionage und nachrichtendienstliche Aktivitäten
- Geostrategische Rivalität
- Sabotage
- Ideologisch oder religiös motivierte Gewalthandlungen
- Staatlich, ideologisch oder religiös motivierte Handlungen
- Sanktionen und wirtschaftliche Zwangsmaßnahmen
- Russland Konfrontation Europa
- Störung der Gasinfrastruktur
- Drohnenangriff
- Cyberkriminalität im engeren Sinn
- Cyberspionage
- Cybersabotage
- Fehlerhafte Software
- Schwerer Industrieunfall mit gefährlichen Stoffen
- Ausfall der Informations- und Kommunikationssysteme für Echtzeitanwendungen
- Technisches Gebrechen
- Blackout

### **Sektor Energie - Teilsektor Wasserstoff:**

- Hochwasser
- Sonstige klimatische bzw. meteorologische Extremereignisse (u.a. rückführbar auf Klimawandel)

---

<sup>109</sup> Die Abkürzung NATECH bedeutet sinngemäß *durch natürliche Gefahren ausgelöste technische Unfälle*.

- Sonstige geologische Extremereignisse (u.a. rückführbar auf Klimawandel)
- Großschadensereignis
- Sabotage
- Spionage und nachrichtendienstliche Aktivitäten
- Cyberkriminalität im engeren Sinn
- Cyberspionage
- Cybersabotage
- Schwerer Industrieunfall mit gefährlichen Stoffen
- Ausfall der Informations- und Kommunikationssysteme für Echtzeitanwendungen
- Technisches Gebrechen
- Blackout
- Drohnenangriff
- NATECH

### **Sektor Energie:**

- Hochwasser
- Dürre
- Sonstige geologische Extremereignisse (u.a. rückführbar auf Klimawandel)
- Abhängigkeiten von ausländischen Technologieanbietern und deren Dienstleistungen
- Fehlendes Fachpersonal
- Rohstoffmangel
- Internet Blackout
- Sabotage
- Spionage und nachrichtendienstliche Aktivitäten
- Ideologisch oder religiös motivierte Gewalthandlungen
- Staatlich, ideologisch oder religiös motivierte Handlungen
- Innentäterschaft
- Störung in der Strominfrastruktur
- Anschlag mit elektromagnetischer Waffe
- Cyberkriminalität im engeren Sinn
- Cyberspionage
- Cybersabotage
- Cyber-Attacke auf kritische IKT-Systeme die physisch mit Stromnetzversorgungsnetzen verbunden sind (Übertragungs-/Verteilernetze, Kraftwerke, Industriebetriebe)
- Fehlerhafte Software
- Drohnenangriff

- Unsichere Hardware
- Ausfall der Informations- und Kommunikationssysteme für Echtzeitanwendungen
- Technisches Gebrechen
- Blackout

#### **Sektor Verkehr - Teilsektor Luftfahrt:**

- Sturm
- Schneemassen
- Sonstige klimatische bzw. meteorologische Extremereignisse (u.a. rückführbar auf Klimawandel)
- Abhängigkeiten von ausländischen Technologieanbietern und deren Dienstleistungen
- Fehlendes Fachpersonal
- Mangelndes Sicherheitsbewusstsein
- Menschliche Fehler (keine Vorsatzhandlungen)
- Störung weltraumbezogener Infrastruktur
- Sabotage
- Spionage und nachrichtendienstliche Aktivitäten
- Drohnenangriff
- Ideologisch oder religiös motivierte Gewalthandlungen
- Staatlich, ideologisch oder religiös motivierte Handlungen
- Militärisch konventioneller Konflikt
- Unbefugter bzw. unkontrollierter Zutritt / Zugriff
- Drohnen
- Anschlag mit elektromagnetischer Waffe
- Cyberkriminalität im engeren Sinn
- Cyberspionage
- Cybersabotage
- Fehlerhafte Software
- Unsichere Hardware
- Unfall in der Luftfahrt
- Serienausfall von Komponenten
- Technisches Gebrechen
- Blackout

#### **Sektor Verkehr - Teilsektor Schienenverkehr:**

- Hochwasser
- Sonstige geologische Extremereignisse (u.a. rückführbar auf Klimawandel)
- Sonstige klimatische bzw. meteorologische Extremereignisse u.a. rückführbar auf Klimawandel)
- Abhängigkeiten von ausländischen Technologieanbietern und deren Dienstleistungen
- Sabotage
- Spionage und nachrichtendienstliche Aktivitäten
- Störung weltraumbezogener Infrastruktur
- Ideologisch oder religiös motivierte Gewalthandlungen
- Staatlich, ideologisch oder religiös motivierte Handlungen
- Störung in der Strominfrastruktur
- Cyberkriminalität im engeren Sinn
- Cyberspionage
- Cybersabotage
- Cyber-Attacke auf kritische IKT-Systeme die physisch mit Stromnetzversorgungsnetzen verbunden sind (Übertragungs-/Verteilernetze, Kraftwerke, Industriebetriebe)
- Fehlerhafte Software
- Serienausfall von Komponenten
- Technisches Gebrechen
- Drohnenangriff
- Blackout

#### **Sektor Verkehr - Teilsektor Schifffahrt:**

- Dürre
- Sonstige geologische Extremereignisse (u.a. rückführbar auf Klimawandel)
- Sonstige klimatische bzw. meteorologische Extremereignisse u.a. rückführbar auf Klimawandel)
- Spionage und nachrichtendienstliche Aktivitäten
- Fehlende Umsetzung oder Mängel im Sicherheitsmanagement
- Mangelndes Sicherheitsbewusstsein
- Menschliche Fehler (keine Vorsatzhandlungen)
- Anstieg Energiepreise
- Drohnenangriff
- Cyberkriminalität im engeren Sinn
- Cyberspionage
- Cybersabotage

- Fehlerhafte Software
- Unfall im Schiffverkehr

### **Sektor Verkehr - Teilsektor Straßenverkehr:**

- Hochwasser
- Schneemassen
- Sonstige geologische Extremereignisse (u.a. rückführbar auf Klimawandel)
- Sonstige klimatische bzw. meteorologische Extremereignisse u.a. rückführbar auf Klimawandel)
- Spionage und nachrichtendienstliche Aktivitäten
- Strommangellage
- Ideologisch oder religiös motivierte Gewalthandlungen
- Staatlich, ideologisch oder religiös motivierte Handlungen
- Störung in der Strominfrastruktur
- Cyberkriminalität im engeren Sinn
- Cyberspionage
- Cybersabotage
- Cyber-Attacke auf kritische IKT-Systeme die physisch mit Stromnetzversorgungsnetzen verbunden sind (Übertragungs-/Verteilernetze, Kraftwerke, Industriebetriebe)
- Ausfall Rechenzentrum
- Ausfall der Informations- und Kommunikationssysteme für Echtzeitanwendungen
- Komplexität der Steuermechanismen im Energiesystem
- Serienausfall von Komponenten
- Blackout
- Drohnenangriff
- NATECH

### **Sektor Verkehr - Teilsektor öffentlicher Verkehr:**

- Hochwasser
- Sonstige geologische Extremereignisse (u.a. rückführbar auf Klimawandel)
- Sonstige klimatische bzw. meteorologische Extremereignisse u.a. rückführbar auf Klimawandel)
- Abhängigkeiten von ausländischen Technologieanbietern und deren Dienstleistungen
- Fehlende Umsetzung oder Mängel im Sicherheitsmanagement
- Mangelndes Sicherheitsbewusstsein

- Sabotage
- Spionage und nachrichtendienstliche Aktivitäten
- Ideologisch oder religiös motivierte Gewalthandlungen
- Staatlich, ideologisch oder religiös motivierte Handlungen
- Störung in der Strominfrastruktur
- Cyberkriminalität im engeren Sinn
- Cyberspionage
- Cybersabotage
- Cyber-Attacke auf kritische IKT-Systeme die physisch mit Stromnetzversorgungsnetzen verbunden sind (Übertragungs-/Verteilernetze, Kraftwerke, Industriebetriebe)
- Cyber-Attacke auf nicht mit dem Stromnetz verbundene Anlagen
- Technisches Gebrechen
- Drohnenangriff
- Blackout

### **Sektor Verkehr:**

- Hochwasser
- Sonstige klimatische bzw. meteorologische Extremereignisse (u.a. rückführbar auf Klimawandel)
- Abhängigkeiten von ausländischen Technologieanbietern und deren Dienstleistungen
- Fehlendes Fachpersonal
- Mangelndes Sicherheitsbewusstsein
- Internet Blackout
- Sabotage
- Spionage und nachrichtendienstliche Aktivitäten
- Ideologisch oder religiös motivierte Gewalthandlungen
- Staatlich, ideologisch oder religiös motivierte Handlungen
- Drohnenangriff
- Anschlag mit elektromagnetischer Waffe
- Cyberkriminalität im engeren Sinn
- Cyberspionage
- Cybersabotage
- Fehlerhafte Software
- Unsichere Hardware
- Ausfall der Informations- und Kommunikationssysteme für Echtzeitanwendungen
- Serienausfall von Komponenten

- Technisches Gebrechen
- Blackout
- NATECH

### **Sektor Bankenwesen:**

- Abhängigkeiten von ausländischen Technologieanbietern und deren Dienstleistungen
- Fehlende Umsetzung oder Mängel im Sicherheitsmanagement
- Finanzmarktkorrektur (Platzen einer Vermögensblase)
- Störung weltraumbezogener Infrastruktur
- Internet Blackout
- Spionage und nachrichtendienstliche Aktivitäten
- Gefahren durch Algorithmen
- Kaskadeneffekt
- Cyberkriminalität im engeren Sinn
- Cyberspionage
- Cybersabotage
- Cyber-Attacke auf kritische IKT-Systeme die physisch mit Stromnetzversorgungsnetzen verbunden sind (Übertragungs-/Verteilernetze, Kraftwerke, Industriebetriebe)
- Ausfall Rechenzentrum
- Ausfall der Informations- und Kommunikationssysteme für Echtzeitanwendungen
- Schäden durch KI-Technologie und Big Data
- Blackout

### **Sektor Finanzmarktinfrastuktur:**

- Abhängigkeiten von ausländischen Technologieanbietern und deren Dienstleistungen
- Fehlendes Fachpersonal
- Störung weltraumbezogener Infrastruktur
- Internet Blackout
- Spionage und nachrichtendienstliche Aktivitäten
- Gefahren durch Algorithmen
- Kaskadeneffekt
- Innentäterschaft
- Cyberkriminalität im engeren Sinn
- Cyberspionage
- Cybersabotage

- Cyber-Attacke auf kritische IKT-Systeme die physisch mit Stromnetzversorgungsnetzen verbunden sind (Übertragungs-/Verteilernetze, Kraftwerke, Industriebetriebe)
- Fehlerhafte Software
- Ausfall Rechenzentrum
- Ausfall der Informations- und Kommunikationssysteme für Echtzeitanwendungen
- Blackout

### Sektor Gesundheit:

- Hochwasser
- Pandemie/Epidemie
- Infektionskrankheiten
- Ausbreitung multiresistenter Keime
- Hitzewellen
- Abhängigkeiten von ausländischen Technologieanbietern und deren Dienstleistungen
- Fehlendes Fachpersonal
- Fehlende Umsetzung oder Mängel im Sicherheitsmanagement
- Störung weltraumbezogener Infrastruktur
- Internet Blackout
- Ausfall Zustell- und Logistikdienste
- Sabotage
- Drohnenangriff
- Spionage und nachrichtendienstliche Aktivitäten
- Ideologisch oder religiös motivierte Gewalthandlungen
- Staatlich, ideologisch oder religiös motivierte Handlungen
- Cyberkriminalität im engeren Sinn
- Cyberspionage
- Cybersabotage
- Cyber-Attacke auf kritische IKT-Systeme die physisch mit Stromnetzversorgungsnetzen verbunden sind (Übertragungs-/Verteilernetze, Kraftwerke, Industriebetriebe)
- Schädigung durch Hyperkonnektivität
- Fehlerhafte Software
- Unsichere Hardware
- Ausfall Rechenzentrum
- Ausfall der Informations- und Kommunikationssysteme für Echtzeitanwendungen
- Technisches Gebrechen
- Blackout

- Drohnenangriff
- NATECH

### **Sektor Trinkwasser:**

- Hochwasser
- Sonstige klimatische bzw. meteorologische Extremereignisse (u.a. rückführbar auf Klimawandel)
- Sonstige geologische Extremereignisse (u.a. rückführbar auf Klimawandel)
- Eutrophierung
- Fehlende Umsetzung oder Mängel im Sicherheitsmanagement
- Mangelndes Sicherheitsbewusstsein
- Strommangellage
- Großschadensereignis
- Stauanlagenbruch
- Altlasten
- Sabotage
- Drohnenangriff
- Spionage und nachrichtendienstliche Aktivitäten
- Ideologisch oder religiös motivierte Gewalthandlungen
- Staatlich, ideologisch oder religiös motivierte Handlungen
- CBRN-Gefahren
- Cyberkriminalität im engeren Sinn
- Cyberspionage
- Cybersabotage
- Cyber-Attacke auf kritische IKT-Systeme die physisch mit Stromnetzversorgungsnetzen verbunden sind (Übertragungs-/Verteilernetze, Kraftwerke, Industriebetriebe)
- Fehlerhafte Software
- Schwerer Industrieunfall mit gefährlichen Stoffen
- Technisches Gebrechen
- Blackout

### **Sektor Abwasser:**

- Hochwasser
- Sonstige klimatische bzw. meteorologische Extremereignisse (u.a. rückführbar auf Klimawandel)

- Sonstige geologische Extremereignisse (u.a. rückführbar auf Klimawandel)
- Menschliche Fehler (keine Vorsatzhandlungen)
- Großschadensereignis
- Sabotage
- Spionage und nachrichtendienstliche Aktivitäten
- CBRN-Gefahren
- Störung in der Strominfrastruktur
- Cyberkriminalität im engeren Sinn
- Cyberspionage
- Cybersabotage
- Drohnenangriff
- Schwerer Industrieunfall mit gefährlichen Stoffen
- Ausfall der Informations- und Kommunikationssysteme für Echtzeitanwendungen
- Technisches Gebrechen
- Blackout

#### **Sektor Digitale Infrastruktur:**

- Hochwasser
- Sturm
- Sonstige klimatische bzw. meteorologische Extremereignisse (u.a. rückführbar auf Klimawandel)
- Sonstige geologische Extremereignisse (u.a. rückführbar auf Klimawandel)
- Sonnenstürme
- Abhängigkeiten von ausländischen Technologieanbietern und deren Dienstleistungen
- Fehlendes Fachpersonal
- Rückstand in Forschung Technologie und Innovation (FTI)
- Störung weltraumbezogener Infrastruktur
- Kaskadeneffekt
- Geostrategische Rivalität
- Sabotage
- Spionage und nachrichtendienstliche Aktivitäten
- Ideologisch oder religiös motivierte Gewalthandlungen
- Staatlich, ideologisch oder religiös motivierte Handlungen
- Sanktionen und wirtschaftliche Zwangsmaßnahmen
- Drohnenangriff
- Anschlag mit elektromagnetischer Waffe

- Cyberkriminalität im engeren Sinn
- Cyberspionage
- Cybersabotage
- Cyber-Attacke auf kritische IKT-Systeme die physisch mit Stromnetzversorgungsnetzen verbunden sind (Übertragungs-/Verteilernetze, Kraftwerke, Industriebetriebe)
- Schädigung durch Hyperkonnektivität
- Fehlerhafte Software
- Unsichere Hardware
- Halbleitermangel
- Ausfall Rechenzentrum
- Ausfall der Informations- und Kommunikationssysteme für Echtzeitanwendungen
- Ausfall Lieferkette
- Blackout
- Ausfall Mobilfunk
- NATECH

### **Sektor Öffentliche Verwaltung:**

- Pandemie/Epidemie
- Infektionskrankheiten
- Mangelndes Sicherheitsbewusstsein
- Menschliche Fehler (keine Vorsatzhandlungen)
- Internet Blackout
- Sabotage
- Spionage und nachrichtendienstliche Aktivitäten
- Staatsfeindliche Verbindungen und demokratieablehnende Szene
- Innentäterschaft
- Subversive Aktivitäten
- Abhängigkeiten von ausländischen Technologieanbietern und deren Dienstleistungen
- Störung in der Strominfrastruktur
- Ausländische Einflussnahme
- Hybride Bedrohungen
- Fehlendes Fachpersonal
- Cyberkriminalität im weiteren Sinn
- Cyberkriminalität im engeren Sinn
- Cyberspionage
- Cybersabotage

- Drohnenangriff
- Blackout

### **Sektor Weltraum:**

- Hochwasser
- Sturm
- Schneemassen
- Sonstige klimatische bzw. meteorologische Extremereignisse (u.a. rückführbar auf Klimawandel)
- Sonstige geologische Extremereignisse (u.a. rückführbar auf Klimawandel)
- Sonnenstürme
- Abhängigkeiten von ausländischen Technologieanbietern und deren Dienstleistungen
- Störung weltraumbezogener Infrastruktur
- Internet Blackout
- Gefahren durch Algorithmen
- Kaskadeneffekt
- Sabotage
- Spionage und nachrichtendienstliche Aktivitäten
- Störung in der Strominfrastruktur
- Cyberkriminalität im engeren Sinn
- Cyberspionage
- Cybersabotage
- Cyber-Attacke auf kritische IKT-Systeme die physisch mit Stromnetzversorgungsnetzen verbunden sind (Übertragungs-/Verteilernetze, Kraftwerke, Industriebetriebe)
- Cyber-Attacke auf nicht mit dem Stromnetz verbundene Anlagen
- Schädigung durch Hyperkonnektivität
- Fehlerhafte Software
- Ausfall Rechenzentrum
- Blackout
- Drohnenangriff
- Ausfall Mobilfunk

### **Produktion, Verarbeitung und Vertrieb von Lebensmitteln:**

- Hochwasser

- Sonstige klimatische bzw. meteorologische Extremereignisse (u.a. rückführbar auf Klimawandel)
- Pandemie/Epidemie
- Hitzewellen
- Kältewelle
- Tierseuche
- Sabotage
- Spionage und nachrichtendienstliche Aktivitäten
- Ausfall Zustell- und Logistikdienste
- Ausfall Lieferkette
- Störung in der Strominfrastruktur
- Blackout
- Internet Blackout
- Gasmangellage
- Desinformation
- CBRN
- Drohnenangriff
- Ausfall von Zahlungsdiensten
- Cyberkriminalität im engeren Sinn
- Cyberspionage
- Cybersabotage

## 6.2 Sektorübergreifenden Auswirkungen

Sektorübergreifende Auswirkungen entstehen dort, wo Störungen in einem Teilsektor nicht auf dessen unmittelbaren Wirkungsbereich begrenzt bleiben, sondern weitere Sektoren in ihrer Funktionsfähigkeit beeinträchtigen. Diese Analyse ist insbesondere für jene Bereiche relevant, deren wesentliche Dienste strukturell voneinander abhängig sind, wie etwa Energie, Verkehr, Gesundheit, digitale Infrastruktur oder öffentliche Verwaltung. Aufgrund dieser engen Verflechtungen besitzen sektorübergreifende Auswirkungen eine besondere Bedeutung für diese Risikoanalyse.

Die Analyse zeigt bereits jetzt, dass einige Teilsektoren eine besonders hohe systemische Relevanz besitzen, da sie als Schlüsselstellen sektorübergreifender Risikoausbreitung fun-

gieren und starke sektorübergreifende Auswirkungen aufweisen. Ein Ausfall der nachfolgenden Sektoren oder Teilsektoren hätte weitreichende Konsequenzen auf andere Sektoren oder Teilsektoren. Dazu zählen unter anderem die Folgenden:

#### **Teilsektor Strom – Sektor Energie:**

Ausfälle führen regelmäßig zu Störungen in allen Sektoren bzw. Teilsektoren, insbesondere in den Sektoren Verkehr, digitale Infrastruktur, öffentliche Verwaltung, Gesundheit, Produktion, Verarbeitung und Vertrieb von Lebensmittel sowie Trinkwasser- und Abwasser.

#### **Sektor Digitale Infrastruktur:**

Störungen in Authentifizierungsdiensten, Cloud-Services, Leit- und Steuerungssystemen oder Datenverbindungen wirken unmittelbar auf nahezu alle Sektoren bzw. Teilsektoren.

#### **Sektor Verkehr:**

Unterbrechungen in Lieferketten beeinflussen die Sektoren Gesundheit, Produktion, Verarbeitung und Vertrieb von Lebensmittel und Energie.

#### **Sektor Öffentliche Verwaltung:**

Beeinträchtigungen führen zu Verzögerungen oder Ausfällen in öffentlichen Aufgaben, die wiederum fast alle anderen Sektoren bzw. Teilsektoren in ihrer Steuerungsfähigkeit betreffen.

#### **Sektoren Trinkwasser bzw. Abwasser:**

Störungen wirken sich unmittelbar auf den Sektor bzw. Teilsektor Gesundheit, Energie und Produktion, Verarbeitung und Vertrieb von Lebensmittel aus.

#### **Sektor Weltraum:**

Störungen von satellitengestützten Diensten wie „global Navigation Satellite System (GNSS)<sup>110</sup>, Satellitenkommunikation oder Zeit- und Synchronisationssignalen können gleichzeitig mehrere Sektoren beeinträchtigen, darunter insbesondere Energie, Verkehr und Finanzmarktinfrastrukturen.

Diese sektorübergreifenden Auswirkungen haben in der aktuellen Bewertung ein erhöhtes Gewicht, da sie häufig Kaskadeneffekte verursachen, die sich über mehrere Sektoren hinweg ausbreiten und deren Ausmaß die Summe der ursprünglichen Störungen deutlich übersteigen kann. Ihr Risikopotenzial wird daher in dieser Risikoanalyse besonders berücksichtigt und prägt die Priorisierung auf gesamtstaatlicher Ebene.

Die in diesem Kapitel vorgenommene Darstellung wird aktualisiert und vertieft, sobald alle Sektoren, Teilsektoren und kritischen Einrichtungen vollständig in den Analyseprozess einbezogen wurden. Erst dann kann die Endfassung der sektorübergreifenden Abhängigkeiten und Risikointeraktionen vorgelegt werden.

### **6.3 Risiken mit grenzüberschreitenden Auswirkungen**

Grenzüberschreitende Risiken umfassen jene Gefahren, deren Ursachen, Ausbreitungswege oder Auswirkungen nicht an den österreichischen Staatsgrenzen enden. Aufgrund der engen wirtschaftlichen, infrastrukturellen und regulatorischen Integration Österreichs in europäische und globale Systeme bestehen in vielen Sektoren starke internationale Abhängigkeiten, die für diese Risikoanalyse von zentraler Bedeutung sind. Dies betrifft insbesondere Energieflüsse, digitale Dienste, Verkehrsverbindungen, Lieferketten und Finanzmarktinfrastrukturen, die alle unmittelbar in überstaatliche Systeme eingebettet sind.

Bereits die bisherigen Erhebungen zeigen jedoch, dass Österreich in mehreren Bereichen erheblichen grenzüberschreitenden Risiken ausgesetzt ist. Dies betrifft etwa potenzielle Störungen oder Ausfälle in den europäischen Elektrizitäts- und Gasnetzen, die bei gleichzeitigen Belastungen oder externen Schocks rasch transnationale Ausmaße annehmen und die heimische Energieversorgung unmittelbar beeinflussen können. Ein grenzüberschreitender

---

<sup>110</sup> GNSS ist ein zusammenfassender Begriff von allen Satellitennavigationssysteme, die weltweit Positionen bestimmen können, wie das bekannte amerikanische GPS, das europäische Galileo, das russische GLONASS und das chinesische BeiDou.

Blackout, der durch Ereignisse in Nachbarländern ausgelöst wird, zählt dabei zu den zentralen Szenarien, da technische Störungen, Extremwetterereignisse oder koordinierte Angriffe im europäischen Verbundnetz weitreichende Auswirkungen in Österreich auslösen können.

Auch Unfälle in kerntechnischen Anlagen (wie Kernkraftwerken) in benachbarten Staaten stellen ein relevantes Risikoszenario dar. Obwohl Österreich selbst keine Kernkraftwerke zur Stromerzeugung betreibt, können Störfälle oder Freisetzungen in Anlagen nahe der Grenze, etwa in der Schweiz, Tschechien, Slowakei, Ungarn oder Slowenien, erhebliche gesundheitliche, ökologische und wirtschaftliche Folgen im österreichischen Staatsgebiet verursachen. Diese Risiken sind aufgrund ihrer potenziellen grenzüberschreitenden Wirkungen besonders zu berücksichtigen.

Darüber hinaus führen natürliche Gefahren mit transnationalem Charakter, wie schwere Stürme, Hochwasserereignisse, Hitzewellen oder großflächige Schneefälle, regelmäßig zu Belastungen mehrerer Staaten gleichzeitig. Besonders ausgeprägt ist dies bei großräumigen Sturm- und Niederschlagsfeldern, die mehrere Staaten gleichzeitig betreffen und die Funktionsfähigkeit technischer Systeme im In- und Ausland beeinträchtigen können.

Auch digitale und wirtschaftliche Abhängigkeiten spielen eine zentrale Rolle. Störungen von Cloud-Diensten, international betriebenen Routing- oder Authentifizierungsdiensten sowie Ausfälle in globalen Liefer- und Produktionsketten entfalten oftmals sofortige Auswirkungen auf österreichische Kommunikationsdienste, das Gesundheitswesen, Produktionsketten oder die öffentliche Verwaltung.

Insgesamt zeigt sich, dass grenzüberschreitende Risiken aufgrund ihrer geografischen Ausbreitung und systemischen Verflechtung das Potenzial besitzen, multiple Sektoren gleichzeitig zu beeinträchtigen und in Österreich ausgeprägte Kaskadeneffekte auszulösen. Die endgültige Bewertung dieser Risiken erfolgt nach Abschluss aller sektoralen Workshops, der vollständigen Datenerhebung und der finalen Identifikation der kritischen Einrichtungen gemäß RKEG.

## **6.4 Klimawandelbedingte Risiken**

Klimawandelbedingte Risiken umfassen jene Gefahren, die durch langfristige Veränderungen des Klimas sowie die Zunahme von Extremereignissen hervorgerufen werden und die

potenziell mehrere Sektoren und Teilsektoren gleichzeitig betreffen. Die bisherigen Ergebnisse dieser Risikoanalyse zeigen, dass Klimawandelwirkungen ein zunehmend dominanter Risikofaktor sind, der in enger Wechselwirkung mit allen Gefahrenkategorien steht. Da Österreich bereits heute von intensiveren Starkniederschlägen, häufigeren Hitzeperioden, erhöhter Waldbrandgefährdung, veränderten Schneehöhen sowie einer steigenden Wahrscheinlichkeit großräumiger Stürme betroffen ist, entstehen umfassende Herausforderungen für kritische Einrichtungen und staatliche Versorgungssysteme.

Klimawandelbedingte Risiken betreffen die österreichischen Sektoren in unterschiedlicher Intensität. Teilsektoren wie Strom und Gas sind vor allem durch Extremwetterereignisse gefährdet, die Leitungsnetze, Umspannwerke oder Speichieranlagen beeinträchtigen können. Der Verkehrssektor sieht sich einer steigenden Belastung durch Hitzeverformungen an Schienen oder Niederschlagsereignisse ausgesetzt, die Infrastrukturabschnitte überregional lahmlegen können. Der Gesundheitssektor ist zunehmend von hitzebedingten Morbiditätsanstiegen und veränderten Infektionsmustern betroffen. Auch die Sektoren Trinkwasser und Abwasser stehen unter Druck, da sowohl längere Trockenperioden als auch Starkregenereignisse die Versorgungssicherheit und Systemstabilität beeinflussen.

Darüber hinaus besitzt der Klimawandel erhebliche potenzielle Auswirkungen auf grenzüberschreitende Infrastrukturen und damit auf die österreichische Risikoexposition. Großflächige Sturmfelder oder Hitzewellen, die mehrere Staaten gleichzeitig betreffen, können etwa Energie- und Verkehrssysteme im Ausland überlasten und über transnationale Abhängigkeiten unmittelbar auf österreichische Teilsektoren zurückwirken. Auch internationale Lieferketten im Gesundheits-, Lebensmittel- oder Energiesektor werden zunehmend stör anfällig, was die Verwundbarkeit stark vernetzter Sektoren weiter erhöht. Diese Verflechtungen verstärken die Notwendigkeit, klimawandelbedingte Risiken nicht nur sektoral, sondern systemisch und grenzüberschreitend zu betrachten.

Bereits im Zwischenstand der vorliegenden Risikoanalyse zeigt sich, dass der Klimawandel als struktureller Treiber anderer Risikokategorien wirkt und bestehende Gefährdungen verstärkt, verlängert oder räumlich ausweitet.

## 6.5 Low Probability/High Impact Risks

Low-Probability/High-Impact-Risks (LPHI) sind seltene, jedoch potenziell katastrophale Ereignisse, deren Auswirkungen aufgrund ihrer Komplexität, Systemrelevanz oder geografischen Reichweite mehrere Sektoren gleichzeitig betreffen können. Dazu zählen etwa großskalige Stromausfälle, Erdbeben mit schweren Auswirkungen, schwere geomagnetische Stürme, nukleare Störfälle in Nachbarstaaten oder extrem unwahrscheinliche, aber folgenschwere technische Systemversagen.<sup>111</sup> Diese Risikokategorie erhält in dieser Risikoanalyse besondere Aufmerksamkeit, da internationale Forschungsergebnisse zeigen, dass LPHI-Ereignisse trotz niedriger Eintrittswahrscheinlichkeiten ein erhebliches gesellschaftliches, wirtschaftliches und infrastrukturelles Schadenspotenzial besitzen.<sup>112</sup>

Die bisher verfügbaren sektoralen Bewertungen weisen darauf hin, dass Österreich durch seine Einbettung in europäische Verbundsysteme, grenzüberschreitende Energie- und Verkehrsinfrastrukturen sowie internationale digitale Dienste in besonderem Maße von seltenen Ereignissen mit hoher Wirkung betroffen sein kann. Studien zeigen zudem, dass Extremereignisse im Bereich des Weltraumwetters, darunter geomagnetische Stürme, die satellitengestützte Dienste beeinträchtigen, zwar selten sind, jedoch potenziell weitreichende Folgen für Navigations-, Kommunikations- und Energiesysteme entfalten können.<sup>113</sup>

Diese Risiken sind deshalb ein zentraler Bestandteil dieser Risikoanalyse, da sie bestehende sektorale Risiken verstärken und in ihren Auswirkungen weit über typische Schadensszenarien hinausreichen können.

## 6.6 Emerging Risks

Emerging Risks umfassen neu auftretende oder sich rasch verändernde Gefahren, deren Eintrittswahrscheinlichkeit und Auswirkungen aufgrund begrenzter Datenlagen oder technologischer, gesellschaftlicher und klimatischer Dynamiken noch nicht abschließend bewertet werden können. Dazu zählen insbesondere Entwicklungen im Bereich künstlicher Intelligenz, digitaler Abhängigkeiten, komplexer Lieferketten, neuer Infektionskrankheiten, Ein-

---

<sup>111</sup> Pescatori, G. / McMillan, L. / Gordon, M. / Aydin, N. Y. / Comes, T. / Maraschini, M. / Palma Oliveira, J. / Terresan, S. / Trump, B. / Pelling, M. / Linkov, I. (2025).

<sup>112</sup> IPCC (2021).

<sup>113</sup> CCAC (2023).

schleppung und Ausbreitung von nicht heimischen Tier- und Pflanzenspezies oder technologischer Systemintegration. Internationale Forschung zeigt, dass Emerging Risks häufig durch ihre Unsicherheit und durch nichtlineare Systemeffekte gekennzeichnet sind, weshalb sie in dieser wie auch anderen staatlichen Risikoanalysen eine zunehmend wichtige Rolle spielen.<sup>114</sup>

Insbesondere neuartige Cyber-Bedrohungen, technologisch bedingte Systeminterdependenzen sowie unvorhersehbare Störungen in globalen Versorgungsketten könnten wesentliche Auswirkungen auf österreichische Sektoren und Teilsektoren entfalten. Emerging Risks sind dadurch gekennzeichnet, dass ihre Relevanz oft erst dann sichtbar wird, wenn bestehende Frühwarnmechanismen oder Risikomodelle an ihre Grenzen stoßen. Studien zeigen, dass solche Risiken häufig unterschätzt werden, insbesondere in hochvernetzten Infrastruktursystemen, in denen geringe Auslöser große systemische Veränderungen hervorrufen können.<sup>115</sup>

Angesichts der hohen Unsicherheit und Dynamik dieser Risikokategorie ist eine fortlaufende Evaluierung wesentlich.

## 6.7 Darstellung der Risikomatrix

Die Risikomatrix stellt das zentrale grafische Instrument dieser Risikoanalyse dar. Sie fasst die zuvor bewerteten Eintrittswahrscheinlichkeiten und Auswirkungen zu einer konsistenten Risikoübersicht für jede Gefahrenkategorie (Naturgefahren, sowie anthropogene-, technische und intentionale Gefahren) zusammen und ermöglicht eine vergleichbare Darstellung der Risikostufen über alle Sektoren hinweg. Gemäß ÖNORM D 4901 müssen die Ergebnisse einer Risikoanalyse nachvollziehbar, transparent und einheitlich aufbereitet werden. Die Matrix dient genau diesem Zweck, indem sie die Risikobewertung in einer zweidimensionalen Struktur abbildet.

Für diese Risikoanalyse wurde eine standardisierte 5×5-Matrix verwendet, die sowohl den Vorgaben der ÖNORM D 4901 als auch den methodischen Prinzipien der ISO 31000 entspricht. Die Eintrittswahrscheinlichkeit wird entlang einer fünfstufigen Skala bewertet, die spezifisch für jede Gefahrenkategorie definiert wurde. Die Auswirkungen orientieren sich

---

<sup>114</sup>Aven T. / Flage, R. (2015a).

<sup>115</sup> World Economic Forum (2024).

an der Verfügbarkeit wesentlicher Dienste gemäß Delegierter Verordnung (EU) 2023/2450 und bilden ebenfalls eine fünfstufige Skala von „sehr gering“ bis „katastrophal“.

In der Risikomatrix werden diese beiden Dimensionen kombiniert, sodass jedes Risiko anhand seiner numerischen Bewertung eindeutig in der Matrix verortet werden kann. Die resultierenden Werte werden zusätzlich in drei farblich unterschiedene Risikobereiche eingeteilt, die eine schnelle Interpretation ermöglichen:

- **Grüner Bereich (niedriges Risiko):**  
Dieser Bereich umfasst Risiken mit geringer Eintrittswahrscheinlichkeit und/oder geringen Auswirkungen. Sie erfordern keine sofortigen Maßnahmen, Monitoring und Beobachtung sind ausreichend. Der grüne Bereich dient als Indikator dafür, dass das Risiko akzeptabel oder bereits angemessen kontrolliert ist.
- **Gelber Bereich (mittleres Risiko):**  
Risiken im gelben Bereich sind relevant und erfordern eine nähere Betrachtung. Hier findet insbesondere eine Kosten-Nutzen-Abwägung statt, um zu bestimmen, ob risikomindernde Maßnahmen verhältnismäßig, wirksam und effizient sind. Der gelbe Bereich zeigt Risiken, die potenziell ansteigen können oder bei denen Maßnahmen sinnvoll, aber nicht zwingend sofort erforderlich sind.
- **Roter Bereich (hohes Risiko):**  
Risiken im roten Bereich weisen eine hohe Eintrittswahrscheinlichkeit, große Auswirkungen oder beides auf. Sie haben hohe Priorität für die staatliche Resilienzplanung und erfordern Maßnahmen, die unmittelbar oder zeitnah zu setzen sind. In der dieser Risikoanalyse bilden diese Risiken den Ausgangspunkt für strategische Handlungsentscheidungen.

Die farbliche Unterteilung dient damit als ergänzende Orientierungshilfe, ersetzt jedoch nicht die fachliche Analyse. Sie unterstützt insbesondere die sektorübergreifende Vergleichbarkeit und die Identifikation jener Risiken, die auf gesamtstaatlicher Ebene besondere Aufmerksamkeit erfordern.

Ein wichtiger Aspekt betrifft die Nichtveröffentlichung der ausgefüllten Risikomatrizen. Da die in dieser Risikoanalyse bewerteten Risiken sicherheitsrelevante Informationen enthalten, unterliegen die befüllten Matrizen dem Schutz vor öffentlicher Einsicht. Es muss sichergestellt werden, dass potenzielle Schwachstellen kritischer Einrichtungen und staatlicher

Systeme nicht offengelegt werden. Aus diesem Grund kann im Rahmen der öffentlichen Dokumentation lediglich eine leere Risikomatrix dargestellt werden, die die grundsätzliche Bewertungslogik und den staatlichen Risikoappetit<sup>116</sup> sichtbar macht, nicht jedoch konkrete Risikopositionen.

Die vollständige Darstellung der verwendeten Skalen sowie die grafische Form der 5×5-Matrix befinden sich im Anhang 3, um eine klare und übersichtliche Präsentation der Bewertungsgrundlagen sicherzustellen.

---

<sup>116</sup> drückt die Bereitschaft einer Person bzw. Institution, Unternehmen oder auch Organisation aus, Risiken einzugehen – nach Wiedemann A. (2000) unter <https://www.gabler-banklexikon.de/definition/risikoappetit-81632/version-380260>. Zugriff am 15.11.2025.

# 7 Dokumentation und Kommunikation

## Anforderungen gemäß ÖNORM D 4901 Normpunkt 10

Die Dokumentation und Kommunikation bilden den abschließenden, aber entscheidenden Schritt dieser nationalen Risikoanalyse. Dieser Schritt stellt sicher, dass die erzielten Ergebnisse nicht nur methodisch nachvollziehbar festgehalten, sondern auch zielgerichtet an die relevanten staatlichen und sektoralen Akteure, bzw. an alle Stakeholder vermittelt werden.

Die ÖNORM D 4901 betont, dass ein Risikomanagementprozess nur dann wirksam ist, wenn seine Resultate transparent dokumentiert, klar kommuniziert und in die jeweiligen Entscheidungsstrukturen eingebettet werden. Für die nationale Risikoanalyse bedeutet dies, dass die ermittelten Risiken, Bewertungen, Kriterien und Ableitungen so aufbereitet sein müssen, dass sie als Grundlage für weitere staatliche Schritte dienen können.

Die Kommunikation der Ergebnisse erfolgt differenziert und zielgruppenorientiert. Das RKEG sieht vor, dass die nationale Risikoanalyse sowohl innerhalb der Bundesregierung als auch gegenüber relevanten Stellen, wie den zuständigen Ressorts, Interessenvertretungen, der Europäischen Kommission sowie kritischen Einrichtungen, kommuniziert wird. Dieser Informationsaustausch stellt sicher, dass die gewonnenen Erkenntnisse in die staatliche Sicherheitsplanung, regulatorische Maßnahmen, zukünftige Lagebilder und die Zusammenarbeit mit der Europäischen Union einfließen.

Ein besonderer Fokus liegt auf der Schnittstelle zwischen dieser Risikoanalyse und den betrieblichen Risikoanalysen der kritischen Einrichtungen. Die Ergebnisse beider Prozesse müssen miteinander kompatibel sein. Die Kommunikation der nationalen Risiken dient daher auch als Referenzrahmen für die kritischen Einrichtungen, damit deren Risikoanalysen inhaltlich anschlussfähig bleiben. Gleichzeitig ermöglicht die strukturierte Kommunikation eine Rückkopplung, durch die neue Erkenntnisse aus den Sektoren wiederum in diese Risikoanalyse einfließen.

Insgesamt sorgt die Dokumentation und Kommunikation dafür, dass die nationale Risikoanalyse ein steuerungsfähiges Instrument bleibt, das sowohl fachlich stringent als auch institutionell wirksam ist. Sie schafft Transparenz, ermöglicht Kooperation und stellt sicher, dass Risikoerkenntnisse nicht im theoretischen Prozess verbleiben, sondern in konkrete staatliche Maßnahmen und strategische Entscheidungen überführt werden.

## 8 Schlussfolgerung und Ausblick

Die nationale Risikoanalyse gemäß RKEG bietet einen systematischen und normbasierten Überblick über jene Risiken, die für die Aufrechterhaltung wesentlicher Dienste in österreichischen kritischen Einrichtungen von zentraler Bedeutung sind. Durch die konsequente Anwendung der ÖNORM Reihe D 4900 und der ISO 31000 ergibt sich ein strukturierter, nachvollziehbarer und reproduzierbarer Prozess, der sowohl die Vielfalt der Gefahren als auch die Komplexität moderner Abhängigkeiten abbildet. Die Ergebnisse verdeutlichen, dass Risiken nicht isoliert entstehen, sondern in einem dynamischen Zusammenspiel aus technologischen, gesellschaftlichen, wirtschaftlichen und geopolitischen Faktoren. Besonders die identifizierten sektorübergreifenden und systemischen Risiken zeigen, wie eng die Funktionsfähigkeit einzelner kritischer Bereiche miteinander verknüpft ist.

Die Analyse bietet nicht nur eine Bestandsaufnahme, sondern bildet auch die Grundlage für strategische Entscheidungen, die in den kommenden Jahren gesetzt werden müssen. Dazu gehören etwa Priorisierungen in der nationalen Strategie für die Resilienz kritischer Einrichtungen, die Weiterentwicklung regulatorischer Rahmenbedingungen oder die gezielte Förderung von Maßnahmen, die die Robustheit und Wiederherstellungsfähigkeit kritischer Einrichtungen stärken.

Der Ausblick verdeutlicht, dass Risikomanagement im staatlichen Kontext ein fortlaufender Prozess ist. Veränderungen in Technologie, Digitalisierung, Klimawandel, geopolitischen Spannungen oder globalen Lieferketten werden die Risikolandschaft in den kommenden Jahren weiter prägen. Daher wird auch diese Risikoanalyse selbst einem kontinuierlichen Monitoring und einer regelmäßigen Überarbeitung unterzogen. Neue Erkenntnisse aus Wissenschaft, Praxis und betrieblichen Risikoanalysen der kritischen Einrichtungen werden schrittweise integriert, um das gesamtstaatliche Risikobild präzise und aktuell zu halten.

Damit schafft die vorliegende Risikoanalyse einen wesentlichen Baustein für die langfristige Stärkung der österreichischen Resilienzarchitektur. Sie ermöglicht es dem Bundesminister für Inneres, Risiken transparent zu priorisieren, vorausschauend zu handeln und jene Maßnahmen zu setzen, die notwendig sind, um die Funktionsfähigkeit zentraler gesellschaftlicher und wirtschaftlicher Strukturen auch in Zukunft sicherzustellen.

# Literaturverzeichnis

**Ackermann, F., & Eden, C.:** Strategic Management of Stakeholders: Theory and Practice. Long Range Planning, 44(3). 2021. <https://doi.org/10.1016/j.lrp.2010.08.001>.

**Alexander, D.** How to Write an Emergency Plan. Liverpool: Liverpool University Press 2016.

**Austrian Standards International:** ÖNORM D 4900: Risikomanagement für Organisationen und Systeme — Begriffe und Grundlagen. Wien. 2021.

**Austrian Standards International:** ÖNORM D 4901: Risikomanagementsysteme – Anforderungen. Wien. 2021a.

**Austrian Standards International:** ÖNORM D 4902-1: Risikomanagement für Organisationen und Systeme — Leitfaden Teil 1: Einbettung des Risikomanagements ins Managementsystem. Wien. 2021b.

**Austrian Standards International :** ÖNORM D 4902-2: Risikomanagement für Organisationen und Systeme — Leitfaden Teil 2: Methoden der Risikobeurteilung. Wien. 2021c.

**Austrian Standards International:** ÖNORM D 4902-3: Risikomanagement für Organisationen und Systeme — Leitfaden Teil 3: Notfall-, Krisen- und Kontinuitätsmanagement. Wien. 2021d.

**Austrian Standards International:** ÖNORM D 4903: Risikomanagement für Organisationen und Systeme — Anforderungen an die Qualifikation des Risikomanagers. Wien. 2021e.

**Aven, T:** Quantitative Risk Assessment: The Scientific Platform. Cambridge: Cambridge University Press. 2011. DOI:10.1017/CBO9780511974120.

**Aven, T.:** Risk Analysis. Wiley. 2015.

**Aven, T. / Flage, R.:** Emerging Risk – Conceptual Definition and a Relation to Black Swan Type of Events. In: Reliability Engineering & System Safety, 144. 2015a. DOI: 10.1016/j.ress.2015.07.008.

**Aven, T.:** Risk Assessment and Risk Management: Review of Recent Advances on Their Foundation. In: European Journal of Operational Research, 253(1). 2016. DOI: 10.1016/j.ejor.2015.12.023.

**BABS – Bundesamt für Bevölkerungsschutz:** Katastrophen- und Notlagen Schweiz (KNS) 2020. Bericht zur nationalen Risikoanalyse. Bern. 2020.

**Baldursson, F. M., Banet, C., & Chyong, C. K.:** Building Resilience in Europe's Energy System. CERRE Report, June 2023. Centre on Regulation in Europe. 2023.

**Bartz, H.-J.:** Entwicklung des klinischen Risikomanagements in deutschen Krankenhäusern / Development of clinical risk management in German hospitals. Bundesgesundheitsblatt – Gesundheitsforschung – Gesundheitsschutz, 65(2). 2021. DOI: 10.1007/s00103-022-03491-5.

**BBK - Bundesamt für Bevölkerungsschutz und Katastrophenhilfe:** 10 Jahre Risikoanalyse im Bevölkerungsschutz Bund. Berlin. 2022.

**BKA - Bundeskanzleramt :** Österreichischen Strategie für Cybersicherheit 2021. Wien. 2021.

**BKA – Bundeskanzleramt:** Österreichische Sicherheitsstrategie 2024. Wien. 2024.

**BKA – Bundeskanzleramt:** Bericht Cybersicherheit für das Jahr 2023. Wien. 2023.

**BMFWF - Bundesministerium für Frauen, Wissenschaft und Forschung:** Österreichs Forschungs- und Technologiebericht. Wien. 2025.

**BMI - Bundeministerium für Inneres:** Staatliches Krisen- und Katastrophenschutzmanagement. Leitfaden – Risikomanagement im Katastrophenmanagement. Wien. 2018. URL: [https://www.bmi.gv.at/204/Download/files/SKKM-Leitfaden\\_fuer\\_das\\_Risikomanagement\\_Version\\_1\\_0.pdf](https://www.bmi.gv.at/204/Download/files/SKKM-Leitfaden_fuer_das_Risikomanagement_Version_1_0.pdf). Zugriff am 13.11.2025.

**BMI - Bundeministerium für Inneres:** Staatliches Krisen- und Katastrophenschutzmanagement. Wien. 2024a. URL: <https://www.bmi.gv.at/204/skkm/>. Zugriff am 14.11.2025.

**BMI - Bundeministerium für Inneres:** Nationale Risikobewertung und Bewertung der Risikomanagementfähigkeiten 2023 (Mitteilung der Republik Österreich gemäß Artikel 6 des Katastrophenschutzverfahrens der Union. Wien. 2024b.

**BMI - Bundesministerium für Inneres:** Staatliches Krisen- und Katastrophenschutzmanagement. Rechtliche und organisatorische Grundlagen. Wien. 2025. URL: [https://www.bmi.gv.at/204/Download/files/186\\_2025\\_SKKM\\_Skriptum\\_V20250917.pdf](https://www.bmi.gv.at/204/Download/files/186_2025_SKKM_Skriptum_V20250917.pdf) Zugriff am 14.11.2025.

**BMK:** Nationale Klimawandelanpassungsstrategie III. Wien. 2023.

**BMK - Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie:** Die Österreichische Strategie zur Anpassung an den Klimawandel. Teil 2 – Aktionsplan. Handlungsempfehlungen für die Umsetzung. Wien. 2024.

**BMK - Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie:** Die Österreichische Strategie zur Anpassung an den Klimawandel. Exekutive Summary. Wien. 2024a.

**BMLUK - Bundesministerium für Land- und Forstwirtschaft, Klima- und Umweltschutz, Regionen und Wasserwirtschaft:** Gefahrenzonenplan Österreich. Wien. 2025. URL: <https://www.gefahrenzonenplan.at>. Zugriff am 25.11.2025.

**Boin, A., Hart, P., Stern, E., & Sundelius, B.:** The Politics of Crisis Management: Public Leadership under Pressure. Cambridge University Press. 2025. DOI: 10.1017/CBO9780511490880.

**Bundesministerium für Landwirtschaft, Forstwirtschaft, Regionen und Wasserwirtschaft:** Austrian Forest Report 2023. Wien. 2023.

**Bryson, J. M.:** What to do when stakeholders matter: Stakeholder identification and analysis techniques. Public Management Review, 6(1). 2004. <https://doi.org/10.1080/14719030410001675722>.

**CCCA - Climate Change Centre Austria:** Klimastatusbericht Österreich 2022. Wien. 2023.

**Christensen, T./Lægreid, P./Rykkja, L. H.:** Organizing for Crisis Management: Building Governance Capacity and Legitimacy. In: Public Administration Review, 2016. <https://doi.org/10.1111/puar.12558>.

**Cox, L. A. T.:** What's wrong with risk matrices? *Risk Analysis*, 28(2), 2008. <https://doi.org/10.1111/j.1539-6924.2008.01030.x>.

**Duchek, S.:** Organizational Resilience: A Capability-Based Conceptualization. In: *Business Research*, 13, 2020, <https://doi.org/10.1007/s40685-019-0085-7>.

**E-Control:** Statistikbroschüre 2023. Wien. 2023.

**EEA - European Environment Agency:** Climate Change, Impacts and Vulnerability in Europe 2016. EEA Report 1/2017. Kopenhagen. 2017.

**EEA - European Environment Agency:** Urban Adaptation to Climate Change in Europe 2.0. Kopenhagen.2020.

**Edwards, P./Bowen, P.:** Risk Management in Project Organisations. Sydney: UNSW Press 2004.

**Europäische Union:** Beschluss Nr. 1313/2013/EU des Europäischen Parlaments und des Rates vom 17. Dezember 2013 über ein Katastrophenschutzverfahren der Union. Amtsblatt L 347. 2013.

**Europäische Union:** Verordnung (EU) 2019/941 des Europäischen Parlaments und des Rates vom 5. Juni 2019 über Risikovorsorge im Elektrizitätssektor und zur Aufhebung der Richtlinie 2005/89/EG. ABl. L 158. 2019.

**Europäische Union:** Richtlinie (EU) 2022/2557 über die Resilienz kritischer Einrichtungen (CER-Richtlinie). Amtsblatt der EU. 2022.

**European Environment Agency:** European Climate Risk Assessment. EEA Report 01/2024. Kopenhagen. 2024.

**European Commission:** Overview of natural and man-made disaster risks the European Union may face – 2020 Edition. Publications Office of the European Union, Luxembourg. 2021. <https://data.europa.eu/doi/10.2795/1521>.

**Frigo, M.L. & Anderson, R.J.:** Strategic Risk Management: A Foundation for Improving Enterprise Risk Management and Governance. *Journal of Corporate Accounting & Finance*, 22(3). 2011. DOI: 10.1002/jcaf.20677.

**Haimes, Y. Y.** (Hg.): Risk Modeling, Assessment, and Management. 4. Aufl. Hoboken: Wiley 2015.

**Hubbard, Douglas W.:** The Failure of Risk Management: Why It's Broken and How to Fix It. John Wiley & Sons, Hoboken. 2020.

**Institut für Föderalismus:** 48. Bericht über den Föderalismus in Österreich. Innsbruck: Institut für Föderalismus. 2023.

**IPCC – Intergovernmental Panel on Climate Change:** Climate Change 2021: The Physical Science Basis. 2021.

**IPCC - Intergovernmental Panel on Climate Change:** Climate Change 2021: The Physical Science Basis. Contribution of Working Group I to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change. Cambridge University Press. 2021. DOI: 10.1017/9781009157896.

**International Organization for Standardization:** ISO 31000:2018 – Risk management – Guidelines. International Organization for Standardization, Genf. 2018.

**Jerab, D. A.:** The Effect of Organizational Structure on Corporate Governance. In: SSRN Electronic Journal. 2023, S. DOI:10.2139/ssrn.4549766.

**Kuipers, S./Wolbers, J.:** Organizational and Institutional Crisis Management. 2021. DOI:10.1093/acrefore/9780190228637.013.1611.

**Leach, W. D., Pelkey, N., & Sabatier, P. A.:** Stakeholder Partnerships as Collaborative Policymaking: Evaluation Criteria Applied to Watershed Management in California and Washington. Journal of Policy Analysis and Management, 21(4). 2002. <https://doi.org/10.1002/pam.10079>.

**Leitch, M.:** ISO 31000:2009 – The New International Standard on Risk Management. In: Risk Analysis. 2010. <https://doi.org/10.1111/j.1539-6924.2010.01397.x>.

**Linkov, I. & Trump, B.D.:** Risk and Resilience: Similarities and Differences. In: The Science and Practice of Resilience. Risk, Systems and Decisions. Springer, Cham. 2019. [https://doi.org/10.1007/978-3-030-04565-4\\_1](https://doi.org/10.1007/978-3-030-04565-4_1).

**Luko, S. N.:** Risk Management Principles and Guidelines. In: Quality Engineering, 2013. DOI: DOI:10.1080/08982112.2013.814508.

**Lundgren, R. E./McMakin, A. H.:** Risk Communication: A Handbook for Communicating Environmental, Safety, and Health Risks. 6. Aufl. Hoboken: Wiley–IEEE Press 2018.

**Monie, S.; Gustafsson, M.; Önnared, S.; Guruvita, K.M.:** Renewable and integrated energy system resilience – A review and generic resilience index. Renewable and Sustainable Energy Reviews. 2025. DOI:10.1016/j.rser.2025.115554.

**OECD:** Managing Emerging Critical Risks: Case Studies and Cross-Country Synthesis Report. OECD Publishing, Paris. 2018. DOI: <https://doi.org/10.1787/1f9858ea-en>.

**Österreichische Raumordnungskonferenz - ÖROK:** 17. Raumordnungsbericht Österreich 2023. Wien. 2023.

**Pescaroli, G. / McMillan, L. / Gordon, M. / Aydin, N. Y. / Comes, T. / Maraschini, M. / Palma Oliveira, J. / Terresan, S. / Trump, B. / Pelling, M. / Linkov, I.:** Definitions and Taxonomy for High Impact Low Probability (HILP) and Outlier Events. In: International Journal of Disaster Risk Reduction. 2025. DOI: 10.1016/j.ijdr.2025.105504.

**Pescaroli, G., & Alexander, D.:** Understanding Compound, Interconnected, Interacting, and Cascading Risks: A Holistic Framework. Risk Analysis. 2018. DOI: 10.1111/risa.13128.

**Petersen, L., Fallou, L., Reilly, P., & Serafinelli, E.:** Critical Infrastructure Operators, Risk Communication and Community Resilience. Conference Paper, 12th International Conference on Structural Safety and Reliability. Wien. 2017.

**Power, M.:** Organized Uncertainty: Designing a World of Risk Management. Oxford: Oxford University Press 2007. DOI:10.1111/j.1467-9299.2008.00756\_2.x.

**Purdy, G.:** ISO 31000:2009 – Setting a New Standard for Risk Management. In: Risk Analysis, 2010. <https://doi.org/10.1111/j.1539-6924.2010.01442.x>.

**Reed, M. S., Graves, A., Dandy, N., Posthumus, H., Hubacek, K., Morris, J., Prell, C., Quinn, C. H., & Stringer, L. C.:** Who's in and Why? A Typology of Stakeholder Analysis Methods for

Natural Resource Management. *Journal of Environmental Management*, 90(5). 2009. <https://doi.org/10.1016/j.jenvman.2009.01.001>.

**Renn, O.:** Risk Governance: Coping With Uncertainty in a Complex World. Ort: Stuttgart, 2008. DOI:10.1007/978-1-4020-6799-0.

**Renn, O.:** Risikogesellschaft und Resilienz: Konzepte für ein integriertes Risikomanagement. Springer VS. 2017.

**Renn, O.:** Systemic Risks in the Anthropocene. *Journal of Risk Research*. 2020. 10.1080/13669877.2020.1779787.

**Rowley, T. J.:** Moving beyond Dyadic Ties: A Network Theory of Stakeholder Influences. *The Academy of Management Review*, 22(4). 1997. <https://doi.org/10.2307/259248>.

**Schulte, Y., Schönefeld, M., Schütte, P. M., & Friedrich, F.:** Crisis Response and Management of Public Administrations: Forgotten Tales. Conference Paper, 21st ISCRAM, Münster. 2024.

**Siegrist, M., Cvetkovich, G., & Roth, C.:** Salient Value Similarity, Social Trust, and Risk/Benefit Perception. *Risk Analysis*, 22(2). 2002. <https://doi.org/10.1111/0272-4332.203034>.

**Statistik Austria:** Statistisches Jahrbuch 2024. Wien. 2024.

**Thaler, T.A., & Hartmann, T.:** Justice and Flood Risk Management: Reflecting on Different Approaches to Distribute and Allocate Flood Risk Management in Europe. *Natural Hazards*, 83(1). 2016. 10.1007/s11069-016-2305-1.

**Thaler, T. A., Priest, S. J., & Fuchs, S.:** Evolving Inter-Regional Co-Operation in Flood Risk Management: Distances and Types of Partnership Approaches in Austria. *Regional Environmental Change*. 2016a. <https://doi.org/10.1007/s10113-015-0796-z>.

**Umweltbundesamt:** Klimaschutzbericht Österreich 2023. Wien. 2023.

**Vesely, W. E., Goldberg, F. F., Roberts, N. H., & Haasi, D. F.:** Fault Tree Handbook. U.S. Nuclear Regulatory Commission. 1981.

**WIFO – Österreichisches Institut für Wirtschaftsforschung:** Bericht zur Wiener Wirtschaft Konjunktur im 1. Halbjahr 2024 und strukturelle Entwicklungen auf mittlere Frist. Wien. 2024.

**World Economic Forum:** Global Risks Report 2024. 19th Edition. Inside Report. 2024. Geneva.

## Abkürzungen

Abb.	Abbildung
Abs.	Absatz
APCIP	Austrian Program for Critical Infrastructure Protection
bspw.	beispielsweise
bzw.	Beziehungsweise
CBRN	chemisch, biologisch, radiologisch und nuklear
EPCIP	European Program for Critical Infrastructure Protection
EU	Europäische Union
ISO	International Organization for Standardization
NATECH	Durch natürliche Gefahren ausgelöste technische Unfälle
ÖNORM	Österreichische Norm
RKEG	Bundesgesetz zur Sicherstellung eines hohen Resilienzniveaus von kritischen Einrichtungen (Resilienz kritischer Einrichtungen-Gesetz)
ua.	Unter anderem

# Anhang 1: Liste der Sektoren inklusive wesentlicher Dienste gemäß Delegierter Verordnung (EU) 2023/2450

Sektor	Teilsektor	Liste wesentlicher Dienste
Energie	Strom	Elektrizitätsversorgung (Elektrizitätsunternehmen);
		Betrieb, Wartung und Ausbau eines Elektrizitätsverteilernetzes (Verteilernetzbetreiber);
		Betrieb, Wartung und Ausbau eines Elektrizitätsübertragungsnetzes (Übertragungsnetzbetreiber);
		Elektrizitätserzeugung (Erzeuger);
		Dienste nominierter Strommarktbetreiber (nominierte Strommarktbetreiber);
		Laststeuerung (Strommarktteilnehmer);
		Aggregation von Elektrizität (Strommarktteilnehmer);
		Energiespeicherung (Strommarktteilnehmer);
	Fernwärme- und -kälte	Bereitstellung von Fernwärme oder -kälte (Betreiber von Fernwärme oder -kälte);
	Erdöl	Fernleitung von Erdöl (Betreiber von Erdöl-Fernleitungen);
		Produktion von Erdöl (Betreiber von Anlagen zur Produktion von Erdöl);
		Raffination und Aufbereitung von Erdöl (Betreiber von Anlagen zur Raffination und Aufbereitung von Erdöl);
		Lagerung von Erdöl (Betreiber von Erdöllagern);

Sektor	Teilsektor	Liste wesentlicher Dienste	
		Verwaltung von Erdölvorräten, einschließlich Notvorräten und spezifischen Erdölvorräten (zentrale Bevorratungsstellen);	
	Erdgas	Lieferung von Erdgas (Versorgungsunternehmen);	
		Verteilung von Erdgas (Verteilernetzbetreiber);	
		Fernleitung von Erdgas (Fernleitungsnetzbetreiber);	
		Speicherung von Erdgas (Betreiber von Speichieranlagen);	
		Betrieb eines Flüssigerdgassystems (Betreiber von LNG-Anlagen);	
		Gewinnung von Erdgas (Erdgasunternehmen);	
		Ankauf von Erdgas (Erdgasunternehmen);	
		Raffination und Aufbereitung von Erdgas (Betreiber von Anlagen zur Raffination und Aufbereitung von Erdgas);	
	Wasserstoff	Erzeugung von Wasserstoff (Betreiber im Bereich Wasserstofferzeugung);	
		Speicherung von Wasserstoff (Betreiber im Bereich Wasserstoffspeicherung);	
		Fernleitung von Wasserstoff (Betreiber im Bereich Wasserstofffernleitung);	
	Verkehr	Luftfahrt	zu gewerblichen Zwecken genutzte Luftverkehrsdienste (Passagiere und Fracht) (Luftfahrtunternehmen);
			Betrieb, Verwaltung und Instandhaltung von Flughäfen und Flughafennetzinfrastruktur (Flughafenleitungsorgane);
Flugverkehrskontrolldienste (Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen);			
Schienenverkehr		Schienenverkehrsdienstleistungen (Passagiere und Fracht) (Eisenbahnunternehmen);	
		Betrieb, Verwaltung und Instandhaltung von Eisenbahninfrastruktur, einschließlich Personenbahnhöfen, Güterterminals, Betriebshöfen und Verkehrskontrollzentren (Infrastrukturbetreiber);	

Sektor	Teilsektor	Liste wesentlicher Dienste	
		Betrieb, Management und Instandhaltung von Schienenverkehr-Serviceeinrichtungen (Betreiber von Serviceeinrichtungen);	
		Betrieb, Verwaltung und Instandhaltung von Systemen für Schienenverkehrsmanagement, Zugsteuerung/ Zugsicherung und Signalgebung sowie von Telekommunikationseinrichtungen und -systemen für die Zugsteuerung, Zugsicherung und Signalgebung (Infrastrukturbetreiber);	
	Schifffahrt	Binnen-, See- und Küstenschifffahrtsdienste (Passagiere und Fracht) (Passagier- und Frachtbeförderungsunternehmen der Binnen-, See- und Küstenschifffahrt);	
		Betrieb, Verwaltung und Instandhaltung von Häfen und Hafenanlagen sowie Betrieb von Einrichtungen, die innerhalb von Häfen befindliche Anlagen und Ausrüstung betreiben, einschließlich Bunkern, Ladungsumschlag, Festmachen, Personenverkehrsdienste, Sammlung von Schiffsabfällen und Ladungsrückständen, Lotsen-, Schleppdienste (Leitungsorgane von Häfen und Einrichtungen, die innerhalb von Häfen befindliche Anlagen und Ausrüstung betreiben);	
		Schiffsverkehrsdienste (Betreiber von Schiffsverkehrsdiensten);	
	Straßenverkehr	Verkehrsmanagementkontrolle, einschließlich Aspekten im Zusammenhang mit der Straßennetzplanung sowie Verkehrsmanagement- und -steuerungsdiensten, mit Ausnahme des Verkehrsmanagements oder des Betriebs intelligenter Verkehrssysteme, sofern sie nicht wesentlicher Bestandteil der allgemeinen Tätigkeit öffentlicher Einrichtungen sind (Straßenverkehrsbehörden);	
		Intelligente Verkehrsdienste (Betreiber intelligenter Verkehrssysteme);	
	öffentlicher Verkehr	öffentliche Personenverkehrsdienste mit der Eisenbahn, anderen Arten des Schienenverkehrs und auf der Straße (Betreiber öffentlicher Dienste);	
	Bankwesen		Entgegennahme von Einlagen (Kreditinstitute);

Sektor	Teilsektor	Liste wesentlicher Dienste
		Kreditvergabe (Kreditinstitute);
Finanzmarkt- infrastruktur		Betrieb eines Handelsplatzes (Betreiber von Handelsplätzen);
		Betrieb von Clearingsystemen (zentrale Gegenparteien);
Gesundheit		Erbringung von Gesundheitsdienstleistungen (Gesundheitsdienstleister);
		Analysen durch ein Referenzlaboratorium der Europäischen Union (EU-Referenzlaboratorien);
		Erforschung und Entwicklung von Arzneimitteln (Einrichtungen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel ausüben);
		Herstellung von pharmazeutischen Grundstoffen und grundlegenden pharmazeutischen Zubereitungen (Einrichtungen, die pharmazeutische Erzeugnisse herstellen);
		Einrichtungen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch eingestuft werden (Einrichtungen, die Medizinprodukte herstellen);
		Vertrieb von Arzneimitteln (Einrichtungen, die eine Großhandelsgenehmigung besitzen);
Trinkwasser		Trinkwasserversorgung und -lieferung unter Ausschluss der Lieferung von Wasser für den menschlichen Gebrauch, sofern dieser Dienst ein nicht wesentlicher Teil der allgemeinen Tätigkeit von Lieferanten anderer Rohstoffe und Güter ist (Lieferanten von und Unternehmen der Versorgung mit Wasser für den menschlichen Gebrauch);

Sektor	Teilsektor	Liste wesentlicher Dienste
Abwasser		Sammlung, Entsorgung und Behandlung von Abwasser mit Ausnahme der Sammlung, Entsorgung oder Behandlung von kommunalem, häuslichem oder industriellem Abwasser, sofern diese Dienste ein nicht wesentlicher Bestandteil der allgemeinen Tätigkeit von Unternehmen sind (Unternehmen, die kommunales, häusliches oder industrielles Abwasser sammeln, entsorgen oder behandeln);
Digitale Infrastruktur		Bereitstellung und Betrieb von Internet-Knoten (Betreiber von Internet-Knoten);
		Erbringung von Diensten für Domänennamensysteme (DNS-Dienste), ausgenommen Dienste im Zusammenhang mit Root-Namenservern (DNS-Diensteanbieter);
		Betrieb und Verwaltung von Namensregistern für Domänen oberster Stufe (TLD-Namenregister);
		Erbringung von Cloud-Computing-Diensten (Anbieter von Cloud-Computing-Diensten);
		Erbringung von Rechenzentrumsdiensten (Anbieter von Rechenzentrumsdiensten);
		Bereitstellung von Inhaltzustellnetzen (Betreiber von Inhaltzustellnetzen);
		Erbringung von Vertrauensdiensten (Vertrauensdiensteanbieter);
		Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste (Anbieter elektronischer Kommunikationsdienste);
		Bereitstellung öffentlicher elektronischer Kommunikationsnetze (Anbieter öffentlicher elektronischer Kommunikationsnetze);

Sektor	Teilsektor	Liste wesentlicher Dienste
öffentliche Verwaltung		Dienstleistungen, die von Einrichtungen der öffentlichen Verwaltung im Sinne von Artikel 2 Nummer 10 der Richtlinie (EU) 2022/2557 von Zentralregierungen entsprechend der jeweiligen Definition der Mitgliedstaaten gemäß nationalem Recht erbracht werden (Einrichtungen der öffentlichen Verwaltung von Zentralregierungen);
Weltraum		Betreiber von Bodeninfrastrukturen, die sich im Eigentum von Mitgliedstaaten oder privaten Parteien befinden und von diesen verwaltet und betrieben werden und die Erbringung von weltraumgestützten Diensten unterstützen, ausgenommen Anbieter öffentlicher elektronischer Kommunikationsnetze (Betreiber von Bodeninfrastrukturen);
Produktion, Verarbeitung und Vertrieb von Lebensmitteln		industrielle Großproduktion und -verarbeitung von Lebensmitteln;
		Lebensmittelkettendienste, einschließlich Lagerung und Logistik;
		Großhandelsvertrieb von Lebensmitteln;

# Anhang 2: Skalierung von Eintrittswahrscheinlichkeit und Auswirkung

## 1 Risikobeurteilung Kategorie „Naturgefahren“

1. unwahrscheinlich	2. selten	3. möglich	4. wahrscheinlich	5. sehr wahrscheinlich
In 300 Jahren nicht nachweislich belegbar	1 x in 300 Jahren	1 x in 100 Jahren	1 x in 10 Jahren	jährlich

## 2 Risikobeurteilung Kategorie „Intentionale Gefahren“

1. unwahrscheinlich	2. selten	3. möglich	4. wahrscheinlich	5. sehr wahrscheinlich
1 x in 12 Jahren	1 x in 6 Jahren	1 x in 3 Jahren	1 x im Jahr	3 x jährlich

## 3 Risikobeurteilung Kategorie „Anthropogene Gefahren“

1. unwahrscheinlich	2. selten	3. möglich	4. wahrscheinlich	5. sehr wahrscheinlich
keine Plausibilität	geringe Plausibilität	plausibel	große Plausibilität	sehr große Plausibilität

## 4 Risikobeurteilung Kategorie „Technische Gefahren“

1. unwahrscheinlich	2. selten	3. möglich	4. wahrscheinlich	5. sehr wahrscheinlich
keine Plausibilität	geringe Plausibilität	plausibel	große Plausibilität	sehr große Plausibilität

## 5 Risikobeurteilung Kategorie „Sektorenübergreifende Abhängigkeiten“

1. unwahrscheinlich	2. selten	3. möglich	4. wahrscheinlich	5. sehr wahrscheinlich
Es ist fast ausgeschlossen - nur unter dem Zusammentreffen von außergewöhnlichen Umständen denkbar, dass ein Ausfall eines Sektors/Teilektors sich auf die Erbringung des eigenen wesentlichen Dienstes auswirkt.	Es ist theoretisch möglich und denkbar, dass ein Ausfall eines Sektors/Teilektors sich auf die Erbringung des eigenen wesentlichen Dienstes auswirkt.	Es ist unter bestimmten Umständen möglich oder <b>maximal einmal</b> im Unternehmen vorgekommen, dass ein Ausfall eines Sektors/Teilektors sich auf die Erbringung des eigenen wesentlichen Dienstes auswirkt.	Es ist bereits <b>mehr als einmal</b> im Unternehmen vorgekommen, dass sich ein Ausfall eines Sektors/Teilektors auf die Erbringung des eigenen wesentlichen Dienstes ausgewirkt hat.	Es tritt regelmäßig oder laufend auf, dass sich ein Ausfall eines Sektors/Teilektors auf die Erbringung des eigenen wesentlichen Dienstes ausgewirkt.

## Skalierung Auswirkung („Verfügbarkeit des wesentlichen Dienstes“)

<p><b>5. katastrophal</b></p>	<p>Der wesentliche Dienst (gem. delegierte VO (EU) 2023/2450) versagt <b>oder</b> ist nur eingeschränkt verfügbar <b>und</b> der meldepflichtige Schwellenwert für Sicherheitsvorfälle gemäß RKEV wird überschritten.</p>	<p>wesentlicher Dienst versagt oder eingeschränkt verfügbar.</p>
<p><b>4. kritisch</b></p>	<p>Der wesentliche Dienst (gem. delegierte VO (EU) 2023/2450) versagt <b>oder</b> ist nur eingeschränkt verfügbar <b>und</b> der meldepflichtige Schwellenwert für Sicherheitsvorfälle gemäß RKEV wird nicht überschritten.</p>	<p>wesentlicher Dienst versagt oder eingeschränkt verfügbar.</p>
<p><b>3. mäßig</b></p>	<p>Der wesentliche Dienst (gem. delegierte VO (EU) 2023/2450) wird beeinträchtigt und kann durch <b>organisationsintern verfügbare und externe zugeführte Ressourcen<sup>1</sup></b> aufrechterhalten werden <b>oder</b> unmittelbar in den Sollzustand<sup>2</sup> zurückversetzt werden.</p>	<p>wesentlicher Dienst droht zu versagen.</p>
<p><b>2. sehr gering</b></p>	<p>Der wesentliche Dienst (gem. delegierte VO (EU) 2023/2450) wird beeinträchtigt und kann durch <b>organisationsintern verfügbare Ressourcen<sup>1</sup></b> bedarfsmäßig aufrechterhalten werden <b>oder</b> bis zu einem nicht-bedrohlichen Zeitraum in den Sollzustand<sup>2</sup> wiederhergestellt werden.</p>	<p>wesentlicher Dienst droht zu versagen.</p>
<p><b>1. gering</b></p>	<p>Der wesentliche Dienst (gem. delegierte VO (EU) 2023/2450) wird beeinträchtigt und kann durch <b>organisationsintern verfügbare Ressourcen<sup>1</sup></b> aufrechterhalten werden <b>oder</b> unmittelbar in den Sollzustand<sup>2</sup> zurückversetzt werden.</p>	<p>wesentlicher Dienst droht zu versagen.</p>

<sup>1</sup> Ressourcen können materiell (Geld, Maschinen, IT, Personal, etc.), immateriell (Know-how), sozial (Netzwerke, Beziehungen) sein

<sup>2</sup> Zustand vor der Bedrohung des wesentlichen Dienstes

# Anhang 3: Risikomatrix

Auswirkung	katastrophal					
	kritisch					
	mäßig					
	gering					
	sehr gering					
		unwahrscheinlich	selten	möglich	wahrscheinlich	Sehr wahrscheinlich
		<b>Wahrscheinlichkeit</b>				

Tabelle Risikomatrix

Auswirkung	Wahrscheinlichkeit				
	unwahrscheinlich	selten	möglich	wahrscheinlich	sehr wahrscheinlich
<b>katastrophal</b>	hoch (rot)	hoch (rot)	hoch (rot)	hoch (rot)	hoch (rot)
<b>kritisch</b>	mittel (gelb)	mittel (gelb)	mittel (gelb)	hoch (rot)	hoch (rot)
<b>mäßig</b>	mittel (gelb)	mittel (gelb)	mittel (gelb)	mittel (gelb)	mittel (gelb)
<b>gering</b>	niedrig (grün)	niedrig (grün)	mittel (gelb)	mittel (gelb)	mittel (gelb)
<b>sehr gering</b>	niedrig (grün)	niedrig (grün)	niedrig (grün)	niedrig (grün)	mittel (gelb)

# Anhang 4: nationaler Gefahrenkatalog

## Naturgefahren

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
1	Hochwasser	N	Hochwasser entsteht, wenn Gewässer wie Flüsse, Bäche oder Wildbäche ihre Ufer überschreiten oder durch Starkregen/Schneesmelze große Wassermengen in kurzer Zeit anfallen (Umweltbundesamt, o.J.).	Ein starkes Hochwasser überflutet eine Anlage, die für die Erbringung des wesentlichen Dienstes essentiell ist.
2	Sturm	N	Ein Sturm ist ein Wind mit einer Stärke von mindestens 9 auf der 12-stufigen Beaufort – Skala. Das entspricht 75 km/h (NÖ Zivilschutzverband, 2008).	Ein Sturm mit einer Stärke von 9 auf der Beaufort-Skala zerstört eine Stromleitung einer Anlage, die für die Erbringung des wesentlichen Dienstes essentiell sind.
3	Erdbeben	N	Ein Erdbeben entsteht durch plötzliche Bewegungen von Erdplatten oder Gesteinsmassen im Erdinneren, wodurch seismische Wellen entstehen, die sich bis zur Erdoberfläche ausbreiten. (Geosphere Austria, o.J.)	Ein Erdbeben beschädigt die Fundamente eines Objektes, die für die Erbringung des wesentlichen Dienstes essentiell sind.
4	Schneemassen	N	Schnee kann in Form von Lawinen oder Schneemassen eine erhebliche Gefahr für Menschen, Gebäude und kritische Infrastruktur darstellen (BMLUK, o.J.)	Eine Lawine zerstört eine Stromleitung einer Anlage, die für die Erbringung des wesentlichen Dienstes essentiell ist.

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
5	Pandemie/ Epidemie	N	Laut dem österreichischen Epidemie-Gesetz 1950 liegt eine Epidemie vor, wenn übertragbare Krankheiten in einer Region gehäuft auftreten und eine ernsthafte Gefahr für die Gesundheit anderer Personen darstellen, sodass behördliche Maßnahmen wie Quarantäne oder Betriebsschließungen notwendig werden. Eine Pandemie wird als Epidemie beschrieben, die sich über Länder- und Kontinentalgrenzen hinweg ausbreitet und große Teile der Bevölkerung betrifft (WHO, 2017).	Eine Pandemie führt zu Personal- bzw. Materialausfällen in einer kritischen Infrastruktur, sowie zu enormen wirtschaftlichen und gesellschaftlichen Konsequenzen. Dadurch kommt es zur Störung bei der Erbringung des wesentlichen Dienstes.
6	Infektionskrankheiten	N	Infektionskrankheiten sind Krankheiten, die durch das Eindringen von Krankheitserregern in den menschlichen Körper und die anschließende Vermehrung im Körper hervorgerufen werden. Man unterscheidet zwischen lokalen oder sich über den ganzen Körper ausbreitenden Infektionskrankheiten, je nachdem ob der Erreger sich nur an der Eintrittspforte vermehrt oder sich über die Blut-beziehungsweise Lymphbahnen im ganzen Körper verbreitet (Stadt Wien, o.J.).	Eine lokale Infektionskrankheit unter den Mitarbeitern einer kritischen Einrichtung führt zu einem Ausfall von Personal und anderen Ressourcen. Dadurch kommt es zur Störung bei der Erbringung des wesentlichen Dienstes.
7	Ausbreitung multiresistenter Keime	N	Diese Bakterien oder Pilze sind gegen mehrere Antibiotika resistent, wodurch Infektionen schwer behandelbar werden (BMASGPK, 2023a).	Eine Infektion mit multiresistenten Bakterien führt zu Personalausfall in einer kritischen Infrastruktur. Dadurch kommt es zur Störung bei der Erbringung des wesentlichen Dienstes.

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
8	Sonstige Klimatische bzw. meteorologische Extremereignisse (u.a. rückführbar auf Klimawandel)	N	Klimatische oder meteorologische Phänomene sind Ereignisse, die den Regelfall bei weitem übersteigen und auf den Klimawandel zurückzuführen sind. Ein Unwetter, einhergehend mit bspw. Überschwemmungen, Hitzewellen, atmosphärisches Blitzeis, Sturm, Hagel oder Tornados ist möglich. Für diese gibt es nur sehr kurze Vorwarnzeiten, jedoch mit räumlicher und zeitlicher Begrenzung. (BMI, 2023a).	Ein Tornado zerstört das Stromnetz einer Anlage, die für die Erbringung des wesentlichen Dienstes essentiell ist.
9	Sonstige Geologische Extremereignisse (u.a. rückführbar auf Klimawandel)	N	Geologische Extremereignisse sind Phänomene, die den Regelfall bei weitem übersteigen und auf den Klimawandel zurückzuführen sind, bspw. gravitative Massenbewegungen worunter man bspw. Felsstürze, Muren Abgänge oder Erdbeben versteht (BMI, 2023a).	Ein Erdbeben beschädigt eine wichtige Straße, die für die Erbringung des wesentlichen Dienstes essentiell ist.
10	Hitzewelle	N	Flächendeckende, intensive und langanhaltende Hitzewellen verursachen Gefahren für kritische Infrastrukturen. Hohe Temperaturen können technische Systeme überhitzen, Kühlanlagen überlasten, den Energiebedarf stark erhöhen sowie die Personalverfügbarkeit reduzieren. Werden Systeme heiß oder versagen Komponenten und Ressourcen, kann dies zu Störungen in der Energieversorgung, den IT-Netzwerken oder bei den Produktionsprozessen führen (BMLUK, 2024).	Eine langanhaltende Hitzewelle überlastet die Kühlanlage eines Systems, das für die Erbringung des wesentlichen Dienstes essentiell ist.

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
11	Kältewelle	N	Eine Kältewelle ist ein Zeitraum von mindestens fünf aufeinanderfolgenden Tagen mit Höchsttemperaturen unter dem Gefrierpunkt, wo an mindestens drei Tagen die Mindesttemperaturen unter -10 Grad (= strenger Frost) liegen (Nationales Krisenzentrum, o.J.).	Eine Kältewelle führt zum Einfrieren der Wasserleitungen in einer Einrichtung einer kritischen Infrastruktur. Dadurch kommt es zur Störung bei der Erbringung des wesentlichen Dienstes.
12	Trockenperiode	N	Eine Trockenperiode ist ein Zeitraum von mehreren Tagen mit sehr geringem Niederschlag (mindestens 5 Tage) mit weniger als 1 mm Niederschlag pro Tag (BMK, 2024).	Eine langanhaltende Trockenperiode führt zu einem Rückgang des Wasserstands in einem Stausee, der für die Erbringung des wesentlichen Dienstes essentiell ist.
13	Dürre	N	Geringe Niederschlagsmengen verursachen einen niedrigen Grundwasserspiegel sowie sinkende Flusststände und haben unmittelbaren Einfluss auf bspw. Trinkwasser, Industrie, Transport und die Lebensmittel-, sowie Energieproduktion (ÖAW, 2023).	Ein niedriger Grundwasserspiegel beeinträchtigt die Wasseraufbereitungsanlagen einer kritischen Infrastruktur. Dadurch kommt es zur Störung bei der Erbringung des wesentlichen Dienstes.
14	Waldbrand	N	Bezeichnet alle unkontrollierten Vegetationsbrände, die abseits von verbauten Gebieten entstehen. Ein Waldbrand wird als unkontrolliertes Feuer definiert, das zumindest teilweise bewaldetes Gebiet erfasst, unabhängig von der Brandart, der Brandfläche und Ursache z. B. auch einzelne, durch Blitzschlag brennende Bäume (EUSALP, 2020).	Ein Waldbrand zerstört die Stromleitungen, die für die Erbringung des wesentlichen Dienstes essentiell sind.

<b>Nr.</b>	<b>Gefahr</b>	<b>Kategorie</b>	<b>Beschreibung</b>	<b>mögliches Szenario</b>
<b>15</b>	Sonnenstürme	N	Durch Sonnenstürme kann es zu in höheren Atmosphären absorbierter Röntgen und UV-Strahlung kommen, welche zu Störungen im Funkverkehr oder in GNSS-Systemen führen (BMI, 2023a).	Ein starker Sonnensturm stört den Funkverkehr einer kritischen Infrastruktur. Dadurch kommt es zur Störung bei der Erbringung des wesentlichen Dienstes.
<b>16</b>	Meteoriteneintritt in die Erdatmosphäre	N	Ein Meteorit in der Größenordnung von über 50 Metern Durchmesser wird als gefährlich eingestuft, da dieser beim Eintritt in die Atmosphäre nicht vollständig zerfällt und dadurch regionale Schäden bis hin zur Beeinträchtigung von kritischen Infrastrukturen verursachen kann (ESA NEO Coordination Centre, o.J.).	Ein Meteorit schlägt in der Nähe einer Anlage einer kritischen Infrastruktur ein und beschädigt den Teil, der für die Erbringung des wesentlichen Dienstes essentiell ist.
<b>17</b>	Eutrophierung	N	Bei Eutrophierung („Überdüngung“) kann es in Gewässern zu massiven Algenblüten kommen, die den Sauerstoffgehalt reduzieren und die Wasserqualität stark verschlechtern (Umweltbundesamt, 2024).	Eine massive Algenblüte in einem Fluss beeinträchtigt die Wasseraufbereitungsanlage, die für die Erbringung eines wesentlichen Dienstes essentiell ist.
<b>18</b>	See-Tsunami nach Bergsturz	N	Durch einen Felssturz oder Bergsturz kann es zu einer See-Tsunamibildung kommen (Bundesamt für Bevölkerungsschutz – BABS, 2023).	Ein Felssturz an einem See löst einen Tsunami aus, der eine Anlage einer kritischen Infrastruktur zerstört. Dadurch kommt es zur Störung bei der Erbringung des wesentlichen Dienstes.

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
19	Tierseuche	N	Ein massenhaftes Auftreten kann zur Tötung großer Tierbestände, zu Handelsbeschränkungen und zu Unterbrechungen in der Nahrungsmittelversorgung führen. Zudem können Transport- und Entsorgungsinfrastrukturen überlastet werden, etwa durch den Abtransport infizierter Tiere oder kontaminierter Materialien (Bundesamt für Bevölkerungsschutz – BABS, 2023).	Ein massenhaftes Auftreten von Tierseuchen führt zu Handelsbeschränkungen, die die Lieferketten eines Lebensmittelunternehmens blockieren. Dadurch kommt es zur Störung bei der Erbringung des wesentlichen Dienstes.

## Anthropogene Gefahren

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
20	Abhängigkeiten von ausländischen Technologieanbietern und deren Dienstleistungen	A	Die Abhängigkeit von ausländischer Technologieanbietern stellt eine zunehmende Gefahr für kritische Infrastrukturen und deren wesentliche Dienste in Österreich dar. Laut der „Strategie zur digitalen Souveränität Österreichs“ des Bundesministeriums für Finanzen bestehen insbesondere in den Bereichen Cloud-Dienste, IT-Sicherheit und Halbleitertechnologien starke Abhängigkeiten von ausländischen Anbietern. Dadurch kann die nationale Handlungsfähigkeit eingeschränkt sein (BMF, 2023). Die Abhängigkeit umfasst auch die Verknappung oder Einschränkung ausländischer Technologien und Dienstleistungen.	Ein ausländischer Anbieter kann eine notwendige Technologie oder Dienstleistung nicht liefern. Dadurch kommt es zur Störung bei der Erbringung des wesentlichen Dienstes.
21	Fehlendes Fachpersonal	A	Fehlendes Fachpersonal stellt eine ernstzunehmende Gefahr für kritische Infrastrukturen und deren wesentliche Dienste dar, da bspw. technische Anlagen, Netzwerke und Versorgungssysteme nur mit qualifizierten Fachkräften betrieben und gewartet werden können. Ein Mangel an IT- und Cybersicherheitsfachkräften gefährdet den Schutz und die Verfügbarkeit von Kommunikations- und Computersystemen (BKA, 2024).	Der Mangel an Fachpersonal führt zu einer Schwachstelle im Netzwerk oder verspäteter Wartung eines Systems, welches für die Erbringung eines wesentlichen Dienstes notwendig ist.

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
22	Fehlende Umsetzung oder Mängel im Sicherheitsmanagement	A	Fehlende oder nur unzureichend vorhandene Umsetzung im Sicherheitsmanagement (Business Continuity Management, Krisenmanagement, Risikomanagement, Konzepte für die physische Sicherheit, Cybersicherheit, Resilienzplan etc.) können im Ereignisfall den Zusammenbruch des wesentlichen Dienstes einer kritischen Infrastruktur verursachen (BMI/BKA, 2017).	Das Fehlen eines funktionierenden Krisenmanagements in einer Krisensituation führt zum kompletten Zusammenbruch des wesentlichen Dienstes.
23	Mangelndes Sicherheitsbewusstsein	A	Ein mangelndes Sicherheitsbewusstsein bezeichnet das unzureichende Bewusstsein von Mitarbeitenden und Organisationen für Gefahren, Gefährdungen, Risiken, sowie erforderliche Schutzmaßnahmen (Onlinesicherheit, 2024).	Ein mangelndes Sicherheitsbewusstsein führt dazu, dass ein:e Mitarbeiter:in Phishing-E-Mails öffnet, welche die IT-Systeme einer kritischen Infrastruktur, die für die Erbringung des wesentlichen Dienstes essentiell sind, gefährdet.
24	Nicht Einhalten von gesetzlichen Rahmenbedingungen	A	Gesetze bilden einen wesentlichen Rahmen für wirtschaftliche Stabilität, fairen Wettbewerb und Nachhaltigkeit aber sind auch Grundlage für zusätzliche finanzielle Aufwendungen bei Neuerungen und/oder Strafzahlungen bei Missmanagement bzw. Gesetzesverstößen (BKA, 2025). Das Nichteinhalten von gesetzlichen Bestimmungen kann zum Entzug von notwendigen Genehmigungen führen und somit den wesentlichen Dienst beeinträchtigen.	Durch eine:n Mitarbeiter:in wird illegal und nicht fachgerecht Müll einer kritischen Infrastruktur entsorgt. Es kommt zu Strafzahlungen bzw. zum Entzug von Genehmigungen, welche die Erbringung des wesentlichen Dienstes stören könnten.

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
25	Zu hohe Verschuldung	A	Ein hoher Verschuldungsgrad (meist mehr als 400% ist als hoch einzustufen, jedoch nach Branche unterschiedlich) kann die Kreditwürdigkeit mindern und sich somit auf die Liquidität auswirken.	Ein hoher Verschuldungsgrad kritischer Infrastruktur führt zu Liquiditätsproblemen, welche die Erbringung des wesentlichen Dienstes stören könnte.
26	Rückstand in Forschung Technologie und Innovation (FTI)	A	Ein technologischer Rückstand, also mangelnde Fortschritte in Forschung, Technologie und Innovation, können für kritische Infrastrukturen und deren wesentliche Dienste gravierende Risiken mit sich bringen. In diesem Kontext bedeutet ein Rückstand, dass wichtige Systeme auf veraltete Technologien angewiesen sind, die weniger leistungsfähig, wartungsintensiver oder anfälliger für Angriffe sind (BMWET, 2025).	Ein technologischer Rückstand führt dazu, dass die Steuerungssysteme einer Anlage, einer kritischen Infrastruktur veraltet sind und ausfallen. Es kommt zur Störung bei der Erbringung des wesentlichen Dienstes.
27	Rohstoffmangel	A	Rohstoffe dienen als Grundlage für die Produktion. Im Masterplan Rohstoffe 2030 werden darunter Baurohstoffe, Metalle, Energieträger und aus Energieträgern produzierte Kunststoffe verstanden. (BMLRT, 2021)	Ein Mangel an wichtigen Metallen führt zu Produktionsausfällen in einer kritischen Infrastruktur. Daraus ergibt sich die Störung bei der Erbringung des wesentlichen Dienstes.

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
28	Gasmangellage	A	Erdgas ist einer der wichtigsten Energieträger Österreichs. Da ein Großteil davon importiert werden muss, besteht eine Abhängigkeit zu anderen Ländern. Aufgrund dieser Importabhängigkeit können u.a. unvorhersehbare politische oder (markt-) technische Ereignisse (plötzliche Nachfragespitzen, politische Unstimmigkeiten in einem Lieferland/Transitland, technisches Versagen etc.) oder witterungsbedingte Extreme (Naturkatastrophen, extreme Winter etc.) zu einer Verschärfung der Gasversorgungssituation führen (BMI, 2023a).	Ein Mangel an Gas als Betriebsmittel führt zu Produktionsausfällen in einer kritischen Infrastruktur. Daraus ergibt sich die Störung bei der Erbringung des wesentlichen Dienstes.
29	Strommangellage	A	Eine Strommangellage tritt ein, wenn zu wenig Strom im Netz verfügbar ist (BMI, 2023a).	Ein Mangel an Strom als Betriebsmittel führt zu Produktionsausfällen in einer kritischen Infrastruktur. Daraus ergibt sich die Störung bei der Erbringung des wesentlichen Dienstes.
30	Mangellage bei Erdöl/-produktion	A	Erdöl und Erdölprodukte sind fossile Energieträger. Da ein Großteil seitens Österreich importiert werden muss, besteht eine Abhängigkeit zu anderen Ländern (BMI, 2023a).	Ein Mangel an Erdöl als Betriebsmittel führt zu Produktionsausfällen in einer kritischen Infrastruktur. Daraus ergibt sich die Störung bei der Erbringung des wesentlichen Dienstes.

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
31	Menschliche Fehler (keine Vorsatzhandlungen)	A	Menschliche Fehler stellen eine der häufigsten Ursachen für Störungen in kritischen Infrastrukturen dar, da sie etwa bei Wartung, Steuerung oder Entscheidungsprozessen usw. zu Fehlfunktionen oder Ausfällen führen können (Umweltbundesamt, 2008).	Ein versehentlicher Wartungsfehler führt zum Ausfall eines wichtigen Systems in einer Anlage einer kritischen Infrastruktur, welches für die Erbringung des wesentlichen Dienstes essentiell ist.
32	Soziale Unzufriedenheit	A	Soziale Unzufriedenheit kann für kritische Infrastrukturen eine ernsthafte Gefahr darstellen, da sie bspw. in Form von Protesten, Streiks etc., zu Unterbrechungen des wesentlichen Dienstes führen kann (BMI/DSN, 2024).	Ein Streik der Mitarbeiter: innen einer kritischen Infrastruktur führt zu Unterbrechungen in der Erbringung des wesentlichen Dienstes.
33	Politische Unstimmigkeit mit dem oder im Zulieferland	A	Politische Unstimmigkeiten im Zulieferland können eine erhebliche Gefahr für kritische Infrastrukturen darstellen, da sie bspw. zu Lieferengpässen, Preisinstabilität oder Unterbrechungen in der Energie- und Rohstoffversorgung führen sowie direkt die Erbringung des wesentlichen Dienstes stören könnten (BMEIA, 2025).	Politische Unstimmigkeiten können beispielsweise zu Unterbrechungen im Schienenverkehr führen und somit zu Lieferengpässen bei einem wichtigen Rohstoff, der für die Erbringung des wesentlichen Dienstes essentiell ist führen.

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
34	Rezession	A	Eine Rezession kann für kritische Infrastrukturen eine erhebliche Gefahr darstellen, da wirtschaftliche Abschwächungen bspw. zu Budgetkürzungen, Personalmangel und Investitionsrückgängen führen können. Dadurch können etwa notwendige Wartungsarbeiten, Modernisierungen und Sicherheitsmaßnahmen verzögert werden, was die Stabilität wesentlicher Dienste gefährdet (WIFO, 2025).	Eine Rezession führt zu Budgetkürzungen in einer kritischen Infrastruktur und stört somit die Erbringung des wesentlichen Dienstes.
35	Anhaltende zu hohe oder zu niedrige Inflation	A	Inflation stellt eine Gefahr für kritische Infrastrukturen dar, da steigende Preise für Energie, Materialien und Personal die Betriebskosten deutlich erhöhen und die Aufrechterhaltung wesentlicher Dienste erschweren könnten. Eine anhaltend hohe Inflation kann die wirtschaftliche Stabilität schwächen und damit auch die Funktionsfähigkeit kritischer Infrastrukturen gefährden (BMSGPK, 2023). Für die Europäische Zentralbank EZB wird eine mittelfristige Inflationsrate von 2 % angestrebt.	Eine hohe Inflation erhöht die Betriebskosten einer kritischen Infrastruktur, wodurch das Erbringen des wesentlichen Dienstes erheblich erschwert ist.

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
36	Finanzmarktkorrektur (Platzen einer Vermögensblase)	A	Das Platzen einer Vermögensblase kann kritische Infrastrukturen gefährden, da es zu bspw. finanziellen Instabilitäten, Liquiditätsengpässen und einem Vertrauensverlust in die Wirtschaft führen könnte. Eine Finanzmarktkorrektur kann erhebliche Auswirkungen auf die Stabilität des Finanzsystems von kritischen Infrastrukturen und die Funktionsfähigkeit wesentlicher Dienste haben (Österreichische Nationalbank, 2022).	Eine Finanzmarktkorrektur führt zu finanziellen Instabilitäten bei einer kritischen Infrastruktur, wobei die Erbringung des wesentlichen Dienstes gestört wird.
37	Unzureichende öffentliche Infrastruktur	A	Mangelhafte Verkehrswege, veraltete Leitungsnetze oder unzuverlässige digitale Infrastruktur führen zu Verzögerungen und erhöhen die Gefahr von Betriebsstörungen in kritischen Infrastrukturen und somit die Erbringung des wesentlichen Dienstes (BMF, 2023).	Veraltete Leitungsnetze führen zu Stromausfällen in einer kritischen Einrichtung. Aufgrund dessen kommt es zu Störungen bei der Erbringung des wesentlichen Dienstes.
38	Störung weltraumbezogener Infrastruktur	A	Eine Störung satellitenbasierter Infrastrukturen betrifft Dienste von Copernicus, dem europäischen Erdbeobachtungssatellitensystem, Positionierungs-, Navigations- und Zeiterfassungsdienste von EGNSS, dem europäischen, globalen Navigationssatellitensystem, sowie Wetterdienste, und satellitenbasierte sichere Kommunikationsdienste. Wenn diese Systeme ausfallen, gestört, blockiert oder manipuliert werden, gefährdet das die Handlungsfähigkeit unseres Staates unmittelbar (BMIMI, 2025).	Eine Störung von Navigationssatelliten beeinträchtigt das Navigationssystem von Fahrzeugen einer kritischen Infrastruktur. Aufgrund dessen kommt es zu Störungen bei der Erbringung des wesentlichen Dienstes.

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
39	Outsourcing von Kernprozessen mit Auswirkungen auf den wesentlichen Dienst	A	Beschreibt die Gefahr, dass sowohl die Kontrolle in Bezug auf die Korrektheit der Abarbeitung der Arbeit, eine Abhängigkeit zu externen Dienstleistern besteht und zugleich Datenschutz und Qualität gefährdet sind (BMI/BKA, 2015).	Die Abhängigkeit von externen IT-Dienstleistern führt zu Datenschutzverletzungen oder Abfluss von sensiblen Daten in einer kritischen Infrastruktur. Aufgrund dessen kommt es zu Störungen bei der Erbringung des wesentlichen Dienstes.
40	Anstieg Energiepreise	A	Kommt es zu einem Anstieg des Energiepreises kann das die Ursache von höheren Betriebskosten für kritische Infrastrukturen bedeuten und ihre finanzielle Stabilität gefährden (Consentec GmbH, 2023).	Ein Anstieg der Energiepreise erhöht die Betriebskosten einer kritischen Infrastruktur, wodurch das Erbringen eines wesentlichen Dienstes einschränkt verfügbar ist.
41	Internet Blackout	A	Ein Internet Blackout, also ein vollständiger oder großflächiger Ausfall von Internetdiensten bedroht kritische Infrastrukturen, weil sie vielfach auf digitale Vernetzung, Cloud-Dienste, Remote-Steuerung und Kommunikationskanäle angewiesen sind. Dadurch kann der wesentliche Dienst nicht mehr zuverlässig erbracht werden, sodass Ausfälle, Verzögerungen und Koordinationsprobleme auftreten können (RTR, 2021).	Ein Internet Blackout führt zu einem Ausfall der Kommunikationssysteme in einer kritischen Infrastruktur. Aufgrund dessen kommt es zu Störungen bei der Erbringung des wesentlichen Dienstes.

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
42	Gefahren durch Algorithmen	A	Durch Gefährdungen, die von Algorithmen (bspw. künstliche Intelligenz) ausgehen (bspw. fehlerhafte Entscheidungen, verzerrte Datenmuster oder Manipulation automatisierter Steuerung), können kritische Infrastrukturen in der Erbringung des wesentlichen Dienstes erheblich gestört werden. Solche algorithmischen Systeme könnten falsche Priorisierungen oder Prognosen treffen und so bspw. Ressourcen falsch zuteilen oder alarmrelevante Signale übersehen (Rechnungshof, 2025).	Eine falsche Entscheidung der künstlichen Intelligenz in einem Versorgungsnetz führt zu falschen Priorisierungen und verursacht Stromausfälle bei kritischen Infrastrukturen. Aufgrund dessen kommt es zu Störungen bei der Erbringung des wesentlichen Dienstes.
43	Erfahrungs-Wissensverlust durch Technik	A	Wenn technologische Systeme moderner Ausprägung dominieren, besteht die Gefahr, dass das traditionelle Erfahrungswissen von Betreibern von kritischen Infrastrukturen (bspw. über manuelle Abläufe, physische Prozesse oder altbewährte Notfallverfahren) in den Hintergrund tritt und mit der Zeit verloren geht. Kritische Infrastrukturen können dadurch anfälliger werden, wenn technische Systeme versagen und kein ausreichendes Wissen vorhanden ist, um manuell oder improvisiert weiterzuarbeiten. Dies kann den wesentlichen Dienst gefährden, weil die Fähigkeit zur Reaktion in Ausnahmesituationen sinkt und alternative Verfahren nicht mehr bekannt sind und nicht mehr geübt werden (BMI/BKA, 2015).	Der Verlust traditionellen Erfahrungswissens führt dazu, dass eine Anlage bei einem technischen Systemausfall nicht mehr manuell betrieben werden kann. Aufgrund dessen kommt es zu Störungen bei der Erbringung des wesentlichen Dienstes.

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
44	Geostrategische Rivalität	A	Die geostrategische Rivalität bezeichnet den Machtwettbewerb zwischen Staaten um politischen, wirtschaftlichen und militärischen Einfluss in einer Region. Diese Rivalität kann zu Störungen globaler Lieferketten führen. In der Folge drohen Unterbrechungen wesentlicher Dienste, was die Stabilität kritischer Infrastrukturen gefährden kann (BMI/DSN, 2025).	Die geostrategische Rivalität zwischen den USA und China führt zu Unterbrechungen in der Lieferkette eines Halbleiterherstellers. Aufgrund dessen kommt es zu Störungen bei der Erbringung des wesentlichen Dienstes in einer kritischen Infrastruktur.
45	Kaskadeneffekt	A	Ein Kaskadeneffekt bezeichnet eine Verkettung von Ausfällen, bei der die Störung einer kritischen Infrastruktur weitere Systeme und Dienste innerhalb der kritischen Infrastruktur beeinträchtigt oder lahmlegt. In komplex vernetzten Infrastrukturen kann ein einzelner Ausfall schnell eine Kette schwerwiegender Folgen auslösen (BMI, 2024b).	Durch einen Mangel an Fachpersonal kommt es zu einem regionalen Stromausfall. Dieser führt zu einem Großbrand in einem Serverzentrum. Das Feuer beschädigt oder zerstört sensible Daten von kritischen Infrastrukturen und somit kommt es zu einer Störung bei der Erbringung des wesentlichen Dienstes.
46	Ausfall Lieferketten	A	Der Ausfall eines oder mehrerer Geschäftspartnern innerhalb einer Lieferkette, kann eine Gefährdung für die Erbringung des wesentlichen Dienstes darstellen, da Lieferketten selbst, Vertriebskanäle, finanzielle Verbindlichkeiten, etc. nicht eingehalten werden können (RTR, 2024).	Der Ausfall eines wichtigen Lieferanten durch Insolvenz führt zu Unterbrechungen in der Produktion in einer kritischen Infrastruktur, was wiederum die Erbringung des wesentlichen Dienstes stört.

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
47	Fehlende wirtschaftliche Chancen / fehlende Märkte	A	Fehlende wirtschaftliche Chancen bzw. fehlende Märkte führen dazu, dass Anbieter in kritischen Infrastrukturen notwendige Investitionen zurückstellen oder sich aus unrentablen Regionen zurückziehen – es drohen Versorgungslücken oder Qualitätsabfall des wesentlichen Dienstes (Landesrechnungshof NÖ, 2022).	Fehlende wirtschaftliche Chancen und Weiterentwicklungen führen dazu, dass eine kritische Infrastruktur sich aus einer ländlichen Region bzw. bestimmtem Gebiet wirtschaftlich zurückzieht. Dadurch entstehen erhebliche Störungen bei der Erbringung des wesentlichen Dienstes in dieser Region.
48	Marktpreisstörungen	A	Marktpreisstörungen, also extreme Preisspitzen, hohe Volatilität oder verzerrte Preisbildung, können Betreiber kritischer Infrastrukturen finanziell unter Druck setzen (Beschaffung, Hedging, Liquidität) und über Lieferantenausstiege bzw. -konzentration die kontinuierliche Erbringung wesentlicher Dienste gefährden (e-Control, 2025).	Extreme Preisspitzen bei Rohstoffen führen zu finanziellen Problemen bei einer kritischen Infrastruktur. Aufgrund dessen kommt es zu Störungen bei der Erbringung des wesentlichen Dienstes.

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
49	sinkende Wettbewerbsfähigkeit	A	Wettbewerbsfähigkeit bezeichnet die Fähigkeit eines Staates oder kritischen Infrastruktur, sich im internationalen wirtschaftlichen Umfeld erfolgreich zu behaupten. Eine sinkende Wettbewerbsfähigkeit kann kritische Infrastrukturen indirekt gefährden, etwa durch Investitionsrückgang, Fachkräftemangel oder Abhängigkeiten von ausländischen Anbietern in der Erbringung des wesentlichen Dienstes (BMI, 2024b).	Eine sinkende Wettbewerbsfähigkeit führt zu einem Investitionsrückgang in der IT-Sicherheit einer kritischen Infrastruktur. Aufgrund dessen kommt es zu Störungen bei der Erbringung des wesentlichen Dienstes.
50	Altlasten	A	Unter Altlasten werden bspw. schadstoffbelastete Böden, Deponien oder kontaminierte Industrieareale verstanden. Diese können Grundwasser, Landwirtschaftsflächen und Siedlungsgebiete verschmutzen. Eine Freisetzung gefährlicher Stoffe, etwa durch Bauarbeiten oder Naturereignisse, kann akute Gesundheits- und Umweltrisiken auslösen. Langfristig führen Altlasten zu hohen Kosten, Nutzungseinschränkungen und einer Gefährdung der Versorgungssicherheit. Somit können Altlasten in diesem Kontext eine schleichende, aber potenziell gravierende Gefahr für kritische Infrastrukturen und deren wesentliche Dienste darstellen (BABS, 2023).	Die Freisetzung von Schadstoffen aus einer kontaminierten Industrieanlage verschmutzt das Grundwasser oder Wasser eines Flusses, das für die Erbringung des wesentlichen Dienstes essentiell ist.

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
51	Ausfall Zustell- und Logistikdienste	A	Zustell- und Logistikdienste sind essentielle Komponenten der Versorgungskette, die den Transport von Waren, bspw. Lebensmitteln, Medikamenten und Betriebsmitteln sicherstellen. Ein Ausfall dieser Dienste kann weitreichende Folgen für kritische Infrastrukturen haben, da Nachschub und Ersatzteile ausbleiben. Ein längerer Ausfall könnte somit die Aufrechterhaltung wesentlicher Dienste gefährden und zu Versorgungsengpässen oder gesellschaftlicher Instabilität führen (BMI, 2024b).	Ein Streik bei einem Logistikunternehmen führt zu einem Ausfall der Lieferungen von Materialien, die für die Erbringung des wesentlichen Dienstes essentiell ist.
52	Ausfall oder Einschränkung in der Abfallentsorgung	A	Ein Ausfall oder eine Einschränkung der Abfallentsorgung kann erhebliche gesundheitliche, ökologische und logistische Folgen haben. Nicht abgeholter oder unsachgemäß gelagerter Abfall führt zur Verbreitung von Krankheitserregern, Schädlingen und unangenehmen Gerüchen, die die öffentliche Hygiene stark beeinträchtigt. Ein länger andauernder Entsorgungsstillstand kann somit die öffentliche Gesundheit, Umweltqualität und Funktionsfähigkeit von kritischen Infrastrukturen gefährden (BABS, 2023).	Ein Streik der regionalen Abfallwirtschafts- und Entsorgungsbetriebe führt zu einer Ansammlung von Abfall, die die Erbringung des wesentlichen Dienstes stören.

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
53	Umweltverschmutzung	A	Umweltverschmutzung stellt eine ernste Gefahr für Gesundheit, Klima und Biodiversität dar. Schadstoffe aus Verkehr, Industrie und Landwirtschaft belasten Luft, Wasser und Böden (Umweltbundesamt, 2025).	Eine starke Luftverschmutzung durch Industrieabfälle beeinträchtigt die Kühlsysteme einer Anlage einer kritischen Infrastruktur. Dadurch kommt es zur Störung bei der Erbringung des wesentlichen Dienstes.

## Intentionale Gefahren

Nr.	Gefahr	Kategorie	Beschreibung	Mögliches Szenario
54	Sabotage	I	Sabotage beschreibt eine Tathandlung, die in böswilliger Absicht durchgeführt wird und eine Schädigung bspw. von Menschen, Maschinen, Arbeitsmitteln oder Produkten herbeiführen kann (z. B.: Racheakt, Brandstiftung, Sachbeschädigung, Vandalismus etc.). Das Motiv ist eine Schädigung und keine Bereicherung (BMI/BKA, 2017).	Ein:e Angreifer:in manipuliert die Steuerungssysteme einer Maschine, die für die Erbringung des wesentlichen Dienstes essentiell ist.
55	Spionage und nachrichtendienstliche Aktivitäten	I	Spionage und nachrichtendienstliche Aktivitäten beschreiben einerseits das Auskundschaften von Geheimnissen durch nachrichtendienstlich gesteuerte Personen oder Gruppen sowie das Auskundschaften von Betriebsgeheimnissen zugunsten der Auftragsnation. (BMI, 2025).	Ein:e Angreifer:in kopiert vertrauliche Daten aus dem Firmennetzwerk, die für die Erbringung des wesentlichen Dienstes essentiell sind.
56	Gewalthandlungen	I	Strafrechtlich relevante Tathandlungen mit Schädigungsabsicht. Dazu werden rechtswidrige Handlungen, mit dem Ziel Menschen zu verletzen, gezählt (z. B.: Drohungen, Amoklauf, etc.) (BMI/BKA, 2017). Gewalthandlungen im Kontext kritischer Infrastrukturen und deren wesentlicher Dienste stellen	Ein:e Angreifer:in legt Feuer in einem Aufenthaltsraum, in dem sich Mitarbeiter:innen, sowie Schlüsselkräfte der kritischen Infrastruktur befinden, welche für die Erbringung des wesentlichen Dienstes essentiell sind, um diese zu verletzen.

Nr.	Gefahr	Kategorie	Beschreibung	Mögliches Szenario
			gezielte physische oder psychische Angriffe dar, die darauf abzielen, Abläufe zu stören, Personal einzuschüchtern oder Infrastruktur zu beschädigen (BMI/DSN, 2025).	
57	Eigentumskriminalität	I	Eigentumskriminalität umfasst alle strafrechtlichen Handlungen mit Bereicherungsabsicht (z. B.: Diebstahl, Einbruch, Erpressung, Raub, etc.) (BMI/BKA, 2017). Für kritische Infrastrukturen bedeutet Eigentumskriminalität, dass technische Anlagen, Gebäude, elektrische Geräte oder Leistungen gestohlen, beschädigt oder zerstört werden können, etwa durch Vandalismus oder gezielte Diebstähle (BMI, 2025).	Ein:e Angreifer:in stiehlt eine wichtige Steuerungseinheit, die für die Erbringung des wesentlichen Dienstes essentiell ist.
58	ideologisch oder religiös motivierte Gewalthandlungen	I	Strafrechtliche Gewalthandlungen mit der Schädigungsabsicht gegen Leib/Leben von Menschen.	Ein:e Angreifer:in verübt bspw. einen ideologisch motiviert Anschlag in oder an einem Objekt um Menschen zu verletzen oder zu töten, wodurch die Erbringung eines wesentlichen Dienstes gestört ist.
59	staatlich, ideologisch oder religiös motivierte Handlungen	I	Widerrechtliche Handlungen, die bspw. die Funktionsfähigkeit von Einrichtungen, Organisationen etc. einschränken (soweit nicht durch Sabotage erfüllt)	Eine Gruppe politisch motivierter Aktivist*innen besetzt bspw. eine Landebahn eines neuralgischen Flughafens

Nr.	Gefahr	Kategorie	Beschreibung	Mögliches Szenario
60	Innentäterschaft	I	Innentäterschaft beschreibt Personen, die bspw. in kritischen Infrastrukturen Informationen entwenden, unautorisiert weitergeben oder andere schädigende Handlungen ausführen. Beschäftigte können auch unbewusst zu Innentätern werden (z.B., wenn sie durch Social Engineering manipuliert werden) (BMI/DSN, 2025).	Ein:e Mitarbeiter:in manipuliert die Steuerungssysteme einer Maschine, die für die Erbringung des wesentlichen Dienstes essentiell sind.
61	Stellvertreterkrieg	I	In einem Stellvertreterkrieg treten Konfliktparteien indirekt gegeneinander an, etwa durch Unterstützung von Proxy-Gruppen in einem Drittland und nutzen territoriale Konflikte als Schlachtfeld für geopolitische Interessen. Solche Konflikte können kritische Infrastrukturen und deren wesentliche Dienste gefährden, wenn sie in Grenzgebieten liegen oder versorgungskritische Wege tangiert werden (BMI/DSN, 2025).	Eine Proxy-Gruppe zerstört ein System, das für die Erbringung des wesentlichen Dienstes essentiell ist.
62	Militärisch konventioneller Konflikt	I	In einem militärisch-konventionellen Konflikt kann der Einsatz bewaffneter Streitkräfte gezielt auf kritische Infrastruktur zielen, um gegnerische Ressourcen, Nachschubwege oder Kommunikationsnetze zu zerstören oder lahmzulegen. (BMI, 2024c).	Bei einer Kampfhandlung wird eine Anlage zerstört, die für die Erbringung des wesentlichen Dienstes essentiell ist.

Nr.	Gefahr	Kategorie	Beschreibung	Mögliches Szenario
63	Organisierte Kriminalität	I	Organisierte Kriminalität umfasst laut dem Bundeskriminalamt Österreich dauerhaft bestehende, hierarchisch strukturierte kriminelle Gruppierungen, die systematisch illegalen Gewinn anstreben; etwa durch Menschenhandel, Drogenhandel, Erpressung oder Insiderdelikte. (BMI, 2024a).	Eine kriminelle organisierte Gruppe zerstört ein System, das für die Erbringung des wesentlichen Dienstes essentiell ist.
64	Sanktionen und wirtschaftliche Zwangsmaßnahmen	I	Sanktionen und wirtschaftliche Zwangsmaßnahmen beschreiben Maßnahmen, die zur Bestrafung oder zur Ausübung von Druck gegen einen Staat, der das Völkerrecht verletzt, angewandt werden können (BMI/DSN, 2022). Einsatz wirtschaftlicher Hebel durch globale oder regionale Mächte, um wirtschaftliche Interaktionen zwischen Nationen umzugestalten, wobei Waren, Wissen, Dienstleistungen oder Technologie eingeschränkt werden, mit dem Ziel, Selbstversorgung zu erreichen, geopolitische Rivalen einzuschränken und/oder Einflussbereiche zu konsolidieren. Dazu gehören, aber sind nicht beschränkt auf: Währungsmaßnahmen, Investitionskontrollen, Sanktionen, staatliche Beihilfen und Subventionen sowie Handelskontrollen. Ergänzend dazu zählen insbesondere Strafzölle zu diesen wirtschaftlichen Maßnahmen. Strafzölle werden gezielt eingesetzt, um	Ein Staat verhängt Strafzölle auf Importe, die für die Erbringung des wesentlichen Dienstes essentiell sind.

Nr.	Gefahr	Kategorie	Beschreibung	Mögliches Szenario
			den Handel mit bestimmten Staaten zu erschweren oder zu sanktionieren, wenn die Staaten Handelsregeln verletzen. Zudem können Strafzölle als politisches Druckmittel dienen (United Nations, 2025).	
65	Subversive Aktivitäten	I	Beschreibt das Bestreben, die Soziale Ordnung in einem Staat negativ zu beeinflussen (z.B. durch Desinformation, Propaganda, gesteuerte Medienkampagnen oder verdeckte Netzwerke). Diese Tathandlung kann bspw. von extremistischen Gruppierungen oder verfeindeten Staaten verfolgt werden (BMI/DSN, 2022 und BMI/DSN, 2025).	Eine extremistische Gruppierung verbreitet Desinformation über eine kritische Infrastruktur, welche einen wesentlichen Dienst betreibt.
66	Russland Konfrontation Europa	I	Laut Verfassungsschutzbericht 2024 wird die „Russland-Konfrontation Europa“ als Teil der aktuellen geopolitischen Spannungen dargestellt, die auch kritische Infrastrukturen und deren wesentliche Dienste betreffen. Der Bericht verweist darauf, dass insbesondere der russische Angriffskrieg gegen die Ukraine und die zunehmende Polarisierung internationaler Beziehungen die Bedrohungslage für Österreich verschärfen. (BMI/DSN, 2025).	Russische Hacker:innen greifen ein sensibles Netzwerk einer kritischen Infrastruktur in Österreich an.
67	Desinformation	I	Beschreibt die gezielte Einflussnahme und Steuerung der öffentlichen Meinung. Dieser Vorgang kann durch	Eine Gruppierung verbreitet gezielt Desinformationen über soziale Medien, die

Nr.	Gefahr	Kategorie	Beschreibung	Mögliches Szenario
			psychologische Beeinflussung, kulturelle und soziale Manipulation oder durch Medien- und Informationsmaßnahmen erfolgen. Ferner gewinnt die Verbreitung von Desinformationen über Soziale Medien und bspw. Deepfake an Bedeutung (BMI/DSN, 2022).	eine kritische Infrastruktur bei der Erbringung eines wesentlichen Dienstes stören.
68	CBRN <sup>117</sup> -Gefahren	I	CBRN – Gefahren ist ein Sammelbegriff für Zwischenfälle, bei denen chemisches, biologisches, radiologisches und nukleare Material vorsätzlich freigesetzt wird (BMI/BKA, 2017).	Ein:e Angreifer:in setzt ein giftiges Gas in einem Lüftungssystem eines Objektes einer kritischen Infrastruktur frei oder legt eine sogenannte „dirty bomb“ mit radioaktiven Material aus, um die Erbringung eines wesentlichen Dienstes zu stören.
69	Störung in der Gasinfrastruktur	I	Eine Störung der Gasinfrastruktur, insbesondere durch vorsätzliche Handlungen gegen bspw. Gasknotenpunkte oder Gasspeicher, stellt eine Gefahr für die Energieversorgung und somit für zahlreiche kritische Infrastrukturen dar (BMI/BKA, 2015).	Ein:e Angreifer:in beschädigt (Vorsatzhandlung) einen Gasspeicher oder Gasknotenpunkt, um die Erbringung des wesentlichen Dienstes einer kritischen Infrastruktur zu stören.
70	Störung in der Strominfrastruktur	I	Eine Störung der Strominfrastruktur durch vorsätzliche Handlungen gegen bspw. Umspannwerke, Hochspannungsleitungen oder Kraftwerke, stellt eine	Ein:e Angreifer:in beschädigt (Vorsatzhandlung) ein Umspannwerk oder eine Hochspannungsleitung, welche für die

<sup>117</sup> chemisch, biologisch, radiologisch und nuklear

Nr.	Gefahr	Kategorie	Beschreibung	Mögliches Szenario
			Gefahr für kritische Infrastrukturen dar (BMI/BKA, 2015).	Erbringung eines wesentlichen Dienstes essentiell sind.
71	Störung in der Ölinfrastruktur	I	Eine Störung der Ölinfrastruktur durch vorsätzliche Handlungen, gegen bspw. Raffinerien, Pipelines oder Tanklagern, gefährdet die Energieversorgung und damit zahlreiche kritische Infrastrukturen (BMI/BKA , 2015).	Ein:e Angreifer:in beschädigt (Vorsatzhandlung) eine Raffinerie oder eine Pipeline, um die Erbringung des wesentlichen Dienstes einer kritischen Infrastruktur zu stören.
72	Drohung gegen Schlüsselkräfte	I	Eine Drohung gegen Schlüsselkräfte im wesentlichen Dienst stellt eine erhebliche Gefahr für die Funktionsfähigkeit kritischer Infrastrukturen dar. Solche Drohungen können bspw. zu Einschüchterung, Arbeitsausfällen oder Sicherheitsrisiken führen und damit die Aufrechterhaltung lebenswichtiger Dienste gefährden (BMI/BKA , 2015).	Eine gefährliche Drohung gemäß StGB gegen eine Schlüsselkraft in einer Einrichtung führt dazu, dass gewisse Leistungen nicht ausgeführt werden können, die für die Erbringung des wesentlichen Dienstes essentiell sind.
73	Ausländische Einflussnahme	I	Ausländische Einflussnahme stellt eine erhebliche Gefahr für kritische Infrastrukturen dar, da sie das Vertrauen in staatliche Institutionen, Medien und öffentliche Dienste schwächen können. Dadurch können Entscheidungsprozesse gestört und gesellschaftliche Spannungen verstärkt werden (BMI, 2024a).	Eine ausländische Macht verbreitet gezielt Desinformationen, die das Vertrauen in die Dienstleistung einer kritischen Infrastruktur, welche einen wesentlichen Dienst erbringt, untergräbt.

Nr.	Gefahr	Kategorie	Beschreibung	Mögliches Szenario
74	Entzug / Manipulation von unternehmensspezifischen Gütern oder Leistungen	I	Wenn gezielt unternehmensspezifische Güter oder Leistungen entzogen oder manipuliert werden, können kritische Infrastrukturen ihre Betriebsprozesse nicht mehr zuverlässig aufrechterhalten. Das kann dazu führen, dass erforderliche Komponenten, Ersatzteile, Software-Updates oder Dienstleistungsinput (z. B. von Logistik-, IT- oder Wartungsanbietern) nicht mehr verfügbar sind oder fehlerhaft geliefert werden.	Ein:e Lieferant:in (Zulieferung) manipuliert wichtige Ersatzteile, die für die Erbringung des wesentlichen Dienstes einer kritischen Infrastruktur, essentiell ist.
75	Unbefugter bzw. unkontrollierter Zutritt / Zugriff	I	Bezeichnet das absichtliche Erlangen von physischem oder digitalem Zugang zu Anlagen, Systemen oder Bereichen kritischer Infrastruktur ohne entsprechende Berechtigung.	Ein:e Angreifer:in dringt unbefugt in eine Anlage einer kritischen Infrastruktur ein, welche für die Erbringung des wesentlichen Dienstes essentiell ist.
76	Juristischer Krieg	I	Unter „juristischer Krieg“ wird die Nutzung rechtlicher Mittel zur Destabilisierung oder Schwächung eines Staates oder Betreibers kritischer Infrastruktur verstanden. Für kritische Infrastrukturen kann das bedeuten, dass sie durch klagebasierte Angriffe, überzogene Regulierung oder Rechtsstreitigkeiten in ihrer Handlungsfähigkeit blockiert werden. Solche Verfahren können Ressourcen (finanziell, personell, juristisch) binden und wichtige Entscheidungen verzögern oder verhindern (BMI, 2024c).	Die Handlungsfähigkeit einer kritischen Infrastruktur, welche einen wesentlichen Dienst erbringt, wird durch überzogene Regulierungen und Rechtsstreitigkeiten absichtlich blockiert.

Nr.	Gefahr	Kategorie	Beschreibung	Mögliches Szenario
77	Drohnenangriff	I	Drohnen können sowohl für zivile als auch für militärische Zwecke genutzt werden und stellen eine Gefahr dar, wenn sie bspw. für Spionage, Schmuggel, Sabotage, Störung im Luftraum, Träger explosiven Materials etc., missbraucht werden (BMI/DSN, 2025).	Eine Drohne wird genutzt, um Aufnahmen vom Areal einer Anlage (Spionage), die einen wesentlichen Dienst erbringt, zu machen.
78	Hybride Bedrohungen	I	Eine „Hybride Bedrohung“ bezeichnet die Kombination unterschiedlicher Mittel und Methoden, um politische oder militärische Ziele zu erreichen (BMLV, 2025).	Ein:e Angreifer:in unterbricht die Energieversorgung einer kritischen Infrastruktur, welche einen wesentlichen Dienst erbringt, und verbreitet gleichzeitig über diese Falschmeldungen in den sozialen Medien.
79	Geopolitik der roten Linien	I	Bezieht sich auf Szenarien, bei denen staatliche oder militärische Akteure Grenzen, Einfluss- oder Versorgungsräume definieren und damit kritische Infrastrukturen gezielt bedrohen oder stören. Eskalationsgrenzen werden dabei immer unklarer. (BMI, 2024c).	Ein Staat blockiert den Zugang zu einem wichtigen Hafen, der für die Erbringung des wesentlichen Dienstes einer kritischen Infrastruktur essentiell ist.
80	Illegaler Handel von nuklearem/radioaktivem Material	I	Diese Gefahr umfasst die unberechtigte Übertragung, den Diebstahl oder den illegalen Verkauf von nuklearen und anderen radioaktiven Materialien. Dadurch können sowohl absichtlich als auch unabsichtlich schwerwiegende Schäden an kritischen Infrastrukturen,	Ein:e Angreifer:in stiehlt radioaktives Material aus einer Anlage einer kritischen Infrastruktur, welche für die Erbringung des wesentlichen Dienstes essentiell ist.

Nr.	Gefahr	Kategorie	Beschreibung	Mögliches Szenario
			Einzelpersonen und der Gesellschaft verursacht und weit verbreitete Kontamination sowie Schäden an Menschen und der Umwelt verursacht werden (Europäische Kommission, 2025).	
81	Anschlag mit elektromagnetischer Waffe	I	Durch die starke elektromagnetische Strahlung durch eine elektromagnetische Waffe (EMP) werden elektronische Systeme, Kommunikationsnetzwerke, Steuerungen und Energieversorgungen zerstört oder dauerhaft gestört (BABS, 2023).	Durch einen Anschlag mittels elektromagnetischer Waffe (EMP) wird ein elektrisches Steuerungssystem, welches für die Erbringung des wesentlichen Dienstes essentiell ist, zerstört.
82	Cyberkriminalität im weiteren Sinn	I	Informations- und Kommunikationstechnik (IKT) als Tatmittel. Hierbei wird diese als Tatmittel zur Vorbereitung, Planung und Ausführung eines herkömmlichen Kriminaldelikts eingesetzt. (BMI, 2025)	Betrugsdelikte ausgeführt über IKT z.B. sog. „CEO-Fraud“, wobei, mittels dem Einsatz von Spoofing und Social-Engineering, Mitarbeiter:innen eines Unternehmens zu einer Geldüberweisung an die Täter:innen verleitet werden.
83	Cyberkriminalität im engeren Sinn	I	Informations- und Kommunikationssysteme (IKT) als Angriffsziel. Hierbei handelt es sich um einen Angriff der sich direkt gegen IKT richtet (BMI, 2025)	Hacking (z.B. Einbringung von Malware in fremde Computersysteme) oder DDoS-Angriffe (z.B. auf Webseiten).
84	Cyberspionage	I	Dieser Begriff fasst Handlungen im Cyberraum zusammen, die der Gewinnung von Informationen oder der Vorbereitung von Angriffen dienen. Dazu zählt die Aufklärung der Struktur von Computernetzwerken	Kompromittierung des Netzwerkes einer kritischen Infrastruktur mit der Absicht das Netzwerk aufzuklären, verdeckte Zugänge anzulegen und Daten zu exfiltrieren.

Nr.	Gefahr	Kategorie	Beschreibung	Mögliches Szenario
			genauso wie das Herstellen und Bereithalten von verdeckten Zugängen in Computersystemen (BMI/DSN, 2025).	
85	Cybersabotage	I	Dieser Begriff beschreibt gezielte, signifikante Angriffe auf Computersysteme, Netzwerke oder Daten, mit der Absicht, die Verfügbarkeit der Ziele zu reduzieren und/oder Daten unerkannt zu manipulieren. Die Täterschaft verfolgt dabei keine eigenen finanziellen Interessen (Abgrenzung zu Ransomware). Sie beabsichtigt vielmehr durch Cybersabotageangriffe eine Schädigung der Interessen verfassungsmäßiger Einrichtungen, der kritischen Infrastruktur oder der Allgemeinheit herbeizuführen (BMI/DSN, 2025).	Eindringen in Computernetzwerke und Löschung der dort vorhandenen Daten sowie die Beschädigung von Operational Technology (OT) durch das bewusste und gezielte Absetzen schädlicher Steuerbefehle.
86	Cyber-Attacke auf kritische IKT-Systeme (Steueranlagen für Übertragungs-/Verteilernetze, Kraftwerke, Industriebetriebe...)	I	Hoher Vernetzungsgrad verschiedener kritischer Infrastrukturen innerhalb Österreichs und Europas, auch zwischen den Sektoren – im Falle eines Angriffes kann das Gesamtsystem beeinträchtigt sein (BMK, 2024).	Ein Cyberangriff auf ein vernetztes Stromnetz beeinträchtigt das Gesamtsystem, das für die Erbringung des wesentlichen Dienstes essentiell ist.
87	Cyber-Attacke auf nicht mit dem	I	Solange keine direkte (physische) Verbindung zum Netzbetrieb besteht, ergibt sich hier keine unmittelbare	Eine systematische Attacke auf die IKT-Systeme einer kritischen Infrastruktur führt

Nr.	Gefahr	Kategorie	Beschreibung	Mögliches Szenario
	Stromnetz verbundene Anlagen		Bedrohung für die Versorgungssicherheit. Eine systematische Attacke auf die IKT-Systeme von Marktteilnehmern kann jedoch mittelbar zu einer kritischen Situation in der Stromversorgung führen (BMK, 2024).	zu einer kritischen Situation in der Stromversorgung, die für die Erbringung des wesentlichen Dienstes essentiell ist.
88	Umweltverschmutzung	I	Umweltverschmutzung stellt eine ernste Gefahr für Gesundheit, Klima und Biodiversität dar. Schadstoffe aus Verkehr, Industrie und Landwirtschaft belasten Luft, Wasser und Böden (Umweltbundesamt, 2025).	Eine starke Luftverschmutzung durch Industrieabfälle beeinträchtigt die Kühlsysteme einer Anlage einer kritischen Infrastruktur. Dadurch kommt es zur Störung bei der Erbringung des wesentlichen Dienstes.
89	Ethno-religiöse Konflikte	I	Ein ethno-religiöser Konflikt entsteht, wenn Spannungen zwischen Gruppen aufgrund ihrer ethnischen Zugehörigkeit und religiösen Unterschiede in offene Feindseligkeiten umschlagen. Solche Konflikte können zu gezielten Angriffen auf kritische Infrastrukturen führen, um Macht auszuüben oder gesellschaftliche Strukturen zu destabilisieren. Dadurch besteht die Gefahr, dass wesentliche Dienste ausfallen und das öffentliche Leben massiv beeinträchtigt wird (BMI/DSN, 2023).	Ein interner oder auch externer ethno-religiöser Konflikt führt zu gezielten Angriffen auf Einrichtungen einer kritischen Infrastruktur. Aufgrund dessen kommt es zu Störungen bei der Erbringung des wesentlichen Dienstes.

Nr.	Gefahr	Kategorie	Beschreibung	Mögliches Szenario
90	Staatsfeindliche Verbindungen und demokratieablehnende Szene	I	Darunter werden Gruppierungen verstanden, welche sich zum Ziel setzen die öffentliche Verwaltung bzw. staatliche Institutionen zu schwächen (BMI/DSN, 2024).	Mitglieder der österreichischen Reichsbürgerideologie weigern sich Steuern zu zahlen und Bescheide anzuerkennen.

## Technische Gefahren

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
91	Schädigung durch Hyperkonnektivität	T	Die steigende digitale Vernetzung von Menschen, Geräten und Systemen führt dazu, dass Störungen in einem Bereich rasch auf andere Systeme übergreifen können. Mehrere wesentliche Dienste können durch einen Kaskadeneffekt gleichzeitig beeinträchtigt werden. Die damit einhergehende größere Anzahl an Vernetzungspunkten und Datenmengen erhöhen die Angriffsfläche für Cyberbedrohungen (BABS, 2023).	Durch die Vernetzung verschiedener digitaler Systeme kommt es zu einer kaskadischen Fehlfunktion im digitalen System, welches für die Erbringung des wesentlichen Dienstes essentiell ist.

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
92	Fehlerhafte, unsichere oder alte Software	T	Software mit bestehenden und bekannten Sicherheitslücken, oder aus bedenklichen Quellen stellt eine Schwachstelle in einem System dar (BMI/BKA, 2017).	Die Nutzung veralteter Software zu denen beispielsweise keine Sicherheitsupdates mehr angeboten werden oder welche keine zeitgemäßen Sicherheitsstandards bieten können, falsch konfigurierter Software (im Sicherheitskontext), sowie Software aus bedenklichen Quellen (nicht offizielle Portale) erhöhen in diesen Einrichtungen die entsprechende Angriffsfläche hinsichtlich Cyberangriffen, welche wiederum die Erbringung des wesentlichen Dienstes stören können.

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
93	Fehlerhafte, unsichere oder alte Hardware	T	Hardware mit bestehenden und bekannten Sicherheitslücken, oder aus bedenklichen Quellen stellt eine Schwachstelle in einem System dar (BMI/BKA, 2017).	Bei Cyberangriffen werden gezielt bestehende Sicherheitslücken im Hardwarebereich ausgenutzt um in fremde Systeme einzudringen. Deshalb sollte die jeweilige Firmware am aktuellsten Stand sein. Hinsichtlich des Ursprunges von Hardware gibt es in anderen Ländern in hoch sensiblen Bereichen teils Verbote gewisser Hardwarekomponenten, aufgrund des Risikos von bewusst platzierten Schwachstellen/Backdoors. Hierdurch ermöglichte Cyberangriffe können wiederum die Erbringung des wesentlichen Dienstes stören.

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
94	Unfall in einem grenznahen Kernkraftwerk	T	Bei Unfällen in grenznahen Kernkraftwerken besteht die Gefahr radioaktiver Kontamination mit Langzeitwirkung (Monate) (BMK, 2024). Da sich das Kernkraftwerk nicht im Inland befindet, kann kein Einfluss auf die direkte Maßnahmensetzung genommen werden. Maßnahmen zum Schutz der Bevölkerung und der Landwirtschaft können, wenn rechtzeitig durchgeführt, die Auswirkungen stark reduzieren. Als grenznah gilt dabei ein Abstand von etwa 200 Kilometern zur österreichischen Grenze (BMI, 2024b).	Ein Leck in einem grenznahen Kernkraftwerk verursacht eine radioaktive Kontamination, die die Verfügbarkeit von Ressourcen einer kritischen Infrastruktur für mehrere Monate beeinträchtigt. Daraus folgt eine Störung bei der Erbringung eines wesentlichen Dienstes.
95	Unfall im Schienenverkehr	T	Unfälle im nationalen und internationalen Schienenverkehr können kritische Infrastrukturen erheblich beeinträchtigen, da sie auf einen zuverlässigen Transport von Material, Personal oder anderen Ressourcen angewiesen sind (BMI/BKA, 2015).	Eine Entgleisung eines Güterzugs auf einer wichtigen Schienenstrecke führt zu einer Blockade der Strecke und unterbricht die Lieferketten für wichtige Ersatzteile, die für die Erbringung des wesentlichen Dienstes essentiell sind.

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
96	Unfall im Schiffverkehr	T	Ein Unfall im nationalen und internationalen Schiffverkehr kann für kritische Infrastrukturen eine Gefahr darstellen, da essentielle Ressourcen nicht transportiert werden können. (BKA/BMI, 2015).	Ein Containerschiff kollidiert mit einer wichtigen Hafeninfrastruktur und verursacht erhebliche Schäden, wodurch die Lieferketten für verschiedene Ressourcen unterbrochen werden, die für die Erbringung des wesentlichen Dienstes essentiell sind.
97	Unfall im Straßenverkehr	T	Ein Unfall im Straßenverkehr kann kritische Infrastrukturen gefährden, indem Versorgungs- und Rettungswege blockiert und somit der Transport von essentiellen Ressourcen oder der Zugang für Einsatzkräfte behindert wird (BMI/BKA, 2015).	Ein Unfall auf einer Hauptverkehrsstraße führt zur Blockade wichtiger Versorgungswege, wodurch der Transport von Ressourcen und der Zugang für Einsatzkräfte behindert wird. Daraus folgt eine Störung bei der Erbringung eines wesentlichen Dienstes.
98	Unfall in der Luftfahrt	T	Ein Unfall in der Luftfahrt stellt eine Gefahr für kritische Infrastrukturen dar, da internationale Lieferketten unterbrochen werden. (BMI/BKA, 2015).	Ein Flugzeugabsturz auf einem wichtigen Flughafen führt zur Schließung der Start- und Landebahnen und unterbricht internationale Lieferketten. Daraus folgt eine Störung bei der Erbringung eines wesentlichen Dienstes.

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
99	Halbleitermangel	T	Beschreibt die mangelnde Verfügbarkeit von Halbleitern am Weltmarkt. Dies ist insofern eine Gefahr, da Mikrochips heutzutage in fast allen technischen Bereichen unverzichtbar geworden sind. Es hat die Folge, dass bei kritischen Infrastrukturen ein Produktionsstillstand zu tragen kommt, kritische Infrastrukturen aufgrund von Lieferkettenunterbrechungen Wartezeiten und höhere Kosten haben, sowie, dass kritische Infrastrukturen ihre Wettbewerbsfähigkeit verlieren und daraus folgernd Arbeitsplätze verloren gehen (BMI/DSN, 2022).	Die mangelnde Verfügbarkeit von Halbleitern führt zu Produktionsstillständen in der Automobilindustrie, was die Lieferketten für wichtige Ersatzteile unterbricht und kritische Infrastrukturen beeinträchtigt, die für die Erbringung wesentlicher Dienste zuständig sind.
100	Ausfall Rechenzentrum	T	Daten oder Prozesse für die Erbringung des wesentlichen Dienstes werden in ein externes Rechenzentrum ausgelagert. Ein Ausfall des Rechenzentrums hat unmittelbare Auswirkungen auf die Erbringung des wesentlichen Dienstes (BMI/DSN, 2022).	Ein schwerer Brand in einem externen Rechenzentrum führt zum vollständigen Datenverlust und unterbricht die Erbringung von Online-Diensten. Daraus folgt eine Störung bei der Erbringung eines wesentlichen Dienstes.

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
101	Schwerer Industrieunfall mit gefährlichen Stoffen	T	Freisetzung gefährlicher Stoffe gem. Seveso III Richtlinie (Richtlinie 2012/18/EU) können Mensch, Umwelt und Infrastruktur unmittelbar gefährden. Die Beherrschung von Gefahren bei Unfällen mit gefährlichen Stoffen erfordert die Einhaltung einer Reihe von gesetzlich vorgeschriebenen Maßnahmen (Amt der Oö. Landesregierung, 2025).	Ein Chemikalienunfall in einem Seveso-Betrieb führt zur Freisetzung giftiger Gase, die die Gesundheit der Bevölkerung und das Personal einer kritischen Infrastruktur gefährden. Dadurch folgt eine Störung bei der Erbringung eines wesentlichen Dienstes.
102	Ausfall der Informations- und Kommunikationssysteme für Echtzeitanwendungen	T	Beschreibt den Verlust der Steuerungsfähigkeit der Anlagen. Es ist keine Datenerfassung und daher keine Früherkennung möglicher Überlastungen gegeben. (BMK, 2024).	Ein Cyberangriff führt zum Verlust der Steuerungsfähigkeit der Anlagen, wodurch keine Datenerfassung und Früherkennung von Überlastungen möglich ist, die für die Erbringung des wesentlichen Dienstes essentiell ist.
103	Komplexität der Steuermechanismen	T	Die zunehmende Komplexität von Steuermechanismen stellt eine wachsende Gefahr für kritische Infrastrukturen dar. Ein Ausfall oder eine Fehlsteuerung kann weitreichende Blackouts, Netzininstabilitäten oder Versorgungsunterbrechungen verursachen (BMI/BKA, 2015).	Eine Fehlsteuerung bspw. bei der Stromverteilung, Trinkwasserverteilung, Abwasserverteilung etc. führt zu einer Netzininstabilität. Dadurch folgt eine Störung bei der Erbringung eines wesentlichen Dienstes.

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
104	Serienausfall von Komponenten	T	Ein Serienausfall von Komponenten kann kritische Infrastrukturen in ihren Grundfunktionen lahmlegen, da viele Systeme gleichzeitig versagen. In einem Energiesystem etwa könnte dies zu großflächigen Stromausfällen, Netzinstabilität und Versorgungsunterbrechungen führen (BMI/BKA, 2015).	Ein Serienausfall von Transformatoren in einem städtischen Stromnetz führt zu großflächigen Stromausfällen und Netzinstabilitäten, die die Erbringung eines wesentlichen Dienstes gefährden.
105	Technisches Gebrechen	T	Ein technisches Gebrechen stellt für kritische Infrastrukturen eine unmittelbare Gefahr dar, da es durch Materialfehler, Systemversagen, menschliches Versagen, oder Wartungsmängel zum Ausfall zentraler Infrastrukturkomponenten führen kann (BMI/BKA, 2015).	Ein Materialfehler in den Turbinen einer kritischen Infrastruktur führt zum plötzlichen Ausfall der Stromerzeugung, die für die Erbringung des wesentlichen Dienstes essentiell ist.
106	Schäden durch KI-Technologie und Big Data	T	KI-Technologie und Big Data können für kritische Infrastrukturen eine Gefahr darstellen, da Fehlfunktionen, Manipulationen oder Datenmissbrauch zu erheblichen Störungen führen können. Eine fehlerhafte oder unkontrollierte Nutzung von KI-Systemen und Big-Data-Analysen kann Entscheidungen automatisierter Infrastrukturen verfälschen und Sicherheitsrisiken erhöhen (BMK, 2021).	Eine fehlerhafte KI-Analyse in einem automatisierten Logistikzentrum führt zu falschen Lagerbestandsdaten und verursacht erhebliche Störungen in der Lieferkette, die für die Erbringung des wesentlichen Dienstes essentiell sind.

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
107	Großflächiger Blackout	T	Durch einen großflächigen und länger andauernden Blackout (kompletter Stromausfall über weite Regionen) verlieren kritische Infrastrukturen ihre Betriebsfähigkeit, sofern keine ausreichenden Notstrom- oder Backupsysteme vorhanden sind. Ohne Strom brechen zentrale technische Funktionen zusammen, wodurch essentielle Dienstleistungen nicht mehr erbracht werden können (BMI, 2022).	Ein großflächiger und länger andauernder Blackout in einer Region führt beispielsweise zum Zusammenbruch der öffentlichen Verkehrsmittel und der Beleuchtung, was die Erbringung eines wesentlichen Dienstes einer kritischen Infrastruktur gefährdet.
108	Ausfall Mobilfunk	T	Ohne funktionierende mobile Kommunikationen können Einsatzkräfte und kritische Infrastrukturen nur eingeschränkt koordiniert werden. Auch Zahlungs-, Transport- und Versorgungssysteme, die auf mobile Netze angewiesen sind, können ausfallen oder stark beeinträchtigt werden. Zudem erschwert der Verlust der Kommunikation die Informationsweitergabe an die Bevölkerung in Krisensituationen (RTR, 2021).	Ein Ausfall des Mobilfunknetzes (Anmerkung: das Mobilfunknetz kann auch durch einen anderen Mobilfunknetzbetreiber nicht wieder hergestellt werden) in einer Region führt zum Zusammenbruch eines Systems, was die Erbringung eines wesentlichen Dienstes einer kritischen Infrastruktur gefährdet.

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
109	Unerwünschte Lastflüsse	T	Unerwünschte Lastflüsse bezeichnen unkontrollierte Stromflüsse im europäischen Verbundnetz, die entstehen, wenn elektrische Energie nicht den vorgesehenen Leitungswegen folgt, etwa durch Netzüberlastungen, Fehlsteuerungen oder Störungen in Nachbarstaaten. Solche Lastflüsse können zu Netzininstabilitäten, Spannungsschwankungen oder im Extremfall zu großflächigen Stromausfällen führen (BMI, 2024b).	Unerwünschte Lastflüsse im europäischen Verbundnetz führen zu Spannungsschwankungen und Netzininstabilitäten. Dadurch folgt eine Störung bei der Erbringung eines wesentlichen Dienstes.
110	NATECH <sup>118</sup>	T	Eine Naturkatastrophe löst zusätzliche technische Schäden oder Störfälle in kritischen Infrastrukturen aus und verschlimmert somit weiter die Katastrophe. (Unece, o.J.).	Ein starkes Erdbeben verursacht Schäden an Stromleitungen und führt zu großflächigen Stromausfällen und Waldbränden. Dadurch folgt eine Störung bei der Erbringung eines wesentlichen Dienstes.
111	Ausfall eines Batteriespeichers	T	Batteriespeicher sind Energiesysteme, die Strom zwischenspeichern um Netzschwankungen auszugleichen und Versorgungssicherheit zu gewährleisten (BMI, 2024b). Durch den Ausfall kann eine Gefahr für die Systemstabilität und somit für den wesentlichen Dienst erfolgen.	Der Ausfall eines großen Batteriespeichers in einer kritischen Infrastruktur führt zu Netzschwankungen und beeinträchtigt die Versorgungssicherheit, und gefährdet somit die Erbringung eines wesentlichen Dienstes.

<sup>118</sup> Die Abkürzung NATECH bedeutet sinngemäß *durch natürliche Gefahren ausgelöste technische Unfälle*

Nr.	Gefahr	Kategorie	Beschreibung	mögliches Szenario
112	Simultaner Ausfall von Hoch- / Höchstspannungskomponenten im Elektrizitätssystem	T	Ein simultaner Ausfall von Hoch-/Höchstspannungskomponenten im Elektrizitätssystem kann zu einer Großstörung oder Stromausfällen führen (BMK, 2024).	Ein simultaner Ausfall von Hochspannungsleitungen in einem regionalen Stromnetz führt zu weitreichenden Stromausfällen und beeinträchtigt die Versorgungssicherheit. Dadurch folgt eine Störung bei der Erbringung eines wesentlichen Dienstes.
113	Stauanlagenbruch	A	Durch einen Stauanlagenbruch kann eine massive Flutwelle ausgelöst werden, welche bspw. kritische Infrastrukturen, Siedlungen und Verkehrswege unter Wasser setzt bzw. die Erbringung des wesentlichen Dienstes hemmt oder sogar aussetzt (BMLUK, 2003).	Ein Stauanlagenbruch löst eine massive Flutwelle aus, die eine Einrichtung einer kritischen Infrastruktur unter Wasser setzt, die für die Erbringung des wesentlichen Dienstes essentiell ist.

