

# **Österreichische Strategie für die Resilienz kritischer Einrichtungen**

ÖSRKE 2026

Wien, 2026

## **Impressum**

Medieninhaber, Verleger und Herausgeber:

Bundesministerium für Inneres, Herrengasse 7, 1010 Wien

Wien, 2026. Stand: 16. 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>4</b>
<b>1 Einleitung</b> .....	<b>5</b>
<b>2 Begriffsbestimmungen</b> .....	<b>8</b>
<b>3 Risikoanalyse</b> .....	<b>10</b>
3.1 Festlegung des Kontexts .....	10
3.2 Der Risikomanagementprozess .....	12
3.3 Kommunikation, Überwachung und Aktualisierung .....	12
3.4 Ergebnisverwendung .....	13
<b>4 Strategische Ausrichtung</b> .....	<b>14</b>
4.1 Strategische Leitlinien.....	15
4.2 Strategische Ziele .....	16
<b>5 Steuerungs- und Koordinationsrahmen</b> .....	<b>18</b>
5.1 Steuerung und Koordination .....	18
5.2 Identifikation kritischer Einrichtungen .....	19
5.3 Auflistung der betroffenen Behörden, beteiligten Bundesministerien, Länder und Interessenvertretungen.....	19
<b>6 Evaluierung und Anpassung</b> .....	<b>21</b>
<b>7 Maßnahmen zur Verbesserung der Resilienz kritischer Einrichtungen</b> .....	<b>23</b>
7.1 Grundsätze der Maßnahmenplanung.....	23
7.2 Maßnahmenkategorien .....	24
7.3 Unterstützung kleiner und mittlerer Unternehmen.....	25
7.4 Zusammenhang Gefahrenkategorien und mögliche Maßnahmen .....	25
<b>8 Koordination und Zusammenarbeit mit dem Bundesamt für Cybersicherheit und die europäische Einbettung</b> .....	<b>27</b>
<b>9 Ausblick</b> .....	<b>29</b>
<b>Quellen- &amp; Literaturverzeichnis</b> .....	<b>30</b>
<b>Abkürzungsverzeichnis</b> .....	<b>33</b>
<b>Anhang 1: Liste der an der Strategie beteiligten Stellen</b> .....	<b>34</b>

# Executive Summary

Die vorliegende nationale Strategie zur Verbesserung der Resilienz kritischer Einrichtungen bildet den zentralen strategischen Rahmen zur Umsetzung des Resilienz kritischer Einrichtungen-Gesetzes (RKEG). Sie orientiert sich an den unionsrechtlichen Vorgaben der Richtlinie (EU) 2022/2557 über die Resilienz kritischer Einrichtungen.

Zunächst enthält die Strategie eine Beschreibung der Risikoanalyse gemäß RKEG, die naturbezogene, technische, anthropogene und intentionale Gefahren, sowie sektorübergreifende und grenzüberschreitende Abhängigkeiten einbezieht. Anschließend werden die strategische Ausrichtung und Zielsetzung festgelegt.

Des Weiteren enthält die Strategie einen Steuerungs- und Koordinationsrahmen, welcher die Umsetzung des RKE-Regimes vorgibt und das Zusammenwirken der handelnden Akteure beschreibt.

Zudem sieht die Strategie eine kontinuierliche Evaluierung und Anpassung vor, die längstens alle vier Jahre erfolgt. Dabei wird die Wirksamkeit der Maßnahmen, die Einbindung der zuständigen Stellen und die Anpassung an neue Risiken und Entwicklungen berücksichtigt. Auf diese Weise soll die Umsetzung der Strategie eine kontinuierliche Verbesserung der Resilienz erwirken.

Abseits dessen legt die Strategie die Grundsätze und Prioritäten der Maßnahmen fest, welche auf der Analyse des nationalen Risikoumfelds beruhen. Die Strategie definiert dabei keine operativen Detailmaßnahmen, sondern beschreibt den übergeordneten Rahmen für die relevanten Akteure.

Zusammenfassend gibt die Strategie einen klar strukturierten, wissenschaftlich fundierten und gesetzeskonformen Rahmen vor, der die Resilienz kritischer Einrichtungen in Österreich nachhaltig stärkt und die Kontinuität wesentlicher gesellschaftlicher und wirtschaftlicher Funktionen sicherstellt.

# 1 Einleitung

Die vorliegende Strategie zur Verbesserung der Resilienz kritischer Einrichtungen der Republik Österreich wird gemäß § 9 Abs. 1 RKEG<sup>1</sup> vom Bundesminister für Inneres vorbereitet und ist von der Bundesregierung zu beschließen. Sie bildet den nationalen, strategischen Rahmen zur Stärkung der Widerstandsfähigkeit jener Einrichtungen, deren Ausfall oder Beeinträchtigung erhebliche Auswirkungen auf die Aufrechterhaltung wesentlicher gesellschaftlicher oder wirtschaftlicher Funktionen hätte.

Das RKEG setzt die RKE-Richtlinie<sup>2</sup> um, welche die Mitgliedstaaten verpflichtet, einheitliche Maßnahmen zur Identifizierung, Bewertung und Absicherung kritischer Einrichtungen zu treffen. Grundlage dieser Richtlinie ist die Annahme, dass die Sicherheit und Funktionsfähigkeit moderner Gesellschaften von grenzüberschreitenden und sektorübergreifenden Abhängigkeiten bestimmt wird. Österreich trägt mit dieser Strategie zur Umsetzung der europäischen Zielvorgaben bei und stärkt gleichzeitig seine nationale Sicherheitsarchitektur.

Zweck dieser Strategie ist es, die in § 9 Abs. 2 RKEG genannten Inhalte in einem kohärenten Rahmen zusammenzuführen. Darin werden die strategischen Ziele festgelegt (Z 1), der Steuerungsrahmen (Z 2) inklusive Koordination beschrieben, Maßnahmen zur Verbesserung der Resilienz einschließlich der zugrundeliegenden Risikoanalyse gemäß § 10 RKEG definiert (Z 3) und das nach § 11 RKEG vorgesehene Verfahren zur Ermittlung kritischer Einrichtungen, ohne dessen Ablauf inhaltlich festzulegen (Z 4), sowie die Unterstützungs- und Vorsorgemaßnahmen gemäß § 13 RKEG benannt (Z 5). Darüber hinaus werden in der Strategie die beteiligten Behörden, Länder und Interessenvertretungen (Z 6) benannt, die Koordination mit dem Bundesamt für Cybersicherheit<sup>3</sup> beschrieben (Z 7) und die Maßnahmen zur Unterstützung kleiner und mittlerer Einrichtungen festgelegt (Z 8).

Die primären Zielgruppen dieser Strategie sind die nach § 11 RKEG als kritisch eingestuften Einrichtungen, sowie die für deren Sektoren zuständigen Bundesministerien und Aufsichts-

---

<sup>1</sup> Bundesgesetz zur Sicherstellung eines hohen Resilienznieaus von kritischen Einrichtungen (Resilienz kritischer Einrichtungen-Gesetz – RKEG), BGBl. I Nr. 60/2025.

<sup>2</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>3</sup> Jene Behörde, welche in Umsetzung des Art. 8 Abs. 1 der Richtlinie (EU) 2555/2022 (NIS-2) als zuständige Behörde benannt wurde.

behörden. Weitere Zielgruppen sind die Länder, Interessenvertretungen und sonstige öffentliche Stellen, die an der Risikoanalyse gemäß § 10 RKEG, an der Ermittlung kritischer Einrichtungen oder an der Umsetzung von Maßnahmen beteiligt sind. Darüber hinaus richtet sich die Strategie an jene nationalen und europäischen Institutionen, für die Berichts- und Informationspflichten im Zusammenhang mit der Resilienz kritischer Einrichtungen bestehen.

Die Strategie folgt einem zyklischen Vorgehen auf Basis des RKEG. Ausgangspunkt ist die Betrachtung der nationalen Risikoanalyse nach § 10 RKEG, in der Gefahren und Abhängigkeiten bewertet werden. Daraus werden gemäß § 9 Abs. 2 Z 1 RKEG strategische Ziele und Prioritäten abgeleitet. Maßnahmen nach § 9 Abs. 2 Z 3–5 RKEG werden risikoorientiert ausgestaltet und durch das Verfahren zur Ermittlung kritischer Einrichtungen nach § 11 RKEG ergänzt. Die Umsetzung erfolgt im Rahmen der Koordinierungs- und Steuerungsprozesse nach § 9 Abs. 2 Z 2, 6 und 7 RKEG. Die regelmäßige Evaluierung nach § 9 Abs. 1 RKEG schließt den strategischen Zyklus.

Die Zuständigkeit für die Koordinierung und Überwachung der Umsetzung dieser Strategie liegt beim Bundesminister für Inneres. Dieser ist zudem zuständige Behörde nach dem RKEG und fungiert als zentrale Anlaufstelle gegenüber den zuständigen Stellen.

Diese Strategie steht in engem Zusammenhang mit der Österreichischen Sicherheitsstrategie 2024<sup>4</sup>, der Nationalen Cybersicherheitsstrategie 2021<sup>5</sup>, dem Österreichischen Programm zum Schutz kritischer Infrastruktur 2014<sup>6</sup> und baut auf diesen, sowie den einschlägigen EU-Regelwerken, auf. Diese werden durch die Strategie um einen sektorübergreifenden Fokus auf physische und organisatorische Resilienz ergänzt.

Ihre Geltungsdauer beträgt längstens vier Jahre. Eine Überprüfung und gegebenenfalls Anpassung kann auch anlassbezogen erfolgen. Der Bundesminister für Inneres berichtet über die Umsetzung und Anpassung dieser Strategie an den Nationalrat (§ 9 Abs. 3 RKEG).

Ziel dieser Strategie ist die Schaffung eines klar strukturierten, wissenschaftlich fundierten und gesetzeskonformen Rahmens, der die Resilienz kritischer Einrichtungen in Österreich

---

<sup>4</sup> <https://www.bundestkanzleramt.gv.at/themen/sicherheitspolitik/sicherheitsstrategie.html> (Zugriff am 13.11.2025).

<sup>5</sup> <https://www.bundestkanzleramt.gv.at/themen/cybersicherheit/oesterreichische-strategie-fuer-cybersicherheit.html> (Zugriff am 14.11.2025).

<sup>6</sup> [Österreichisches Programm zum Schutz kritischer Infrastrukturen \(APCIP\)](#) (Zugriff am 14.11.2025).

nachhaltig stärkt, sektorübergreifende Zusammenarbeit fördert und die Grundlage für ein hohes Maß an Versorgungssicherheit und gesellschaftlicher Widerstandsfähigkeit bildet.

## 2 Begriffsbestimmungen

Um sicherzustellen, dass die Strategie eine einheitliche, standardkonforme Terminologie verwendet, die sowohl rechtlich als auch technisch den Stand der Wissenschaft und Technik widerspiegelt, entsprechen die in dieser Strategie verwendeten Begriffe den Legaldefinitionen des § 3 RKEG. Soweit in dieser Strategie Begriffe wie „kritische Einrichtung“, „wesentlicher Dienst“ oder „Resilienz“, etc. verwendet werden, gelten die dort festgelegten Begriffsbestimmungen.

**„Beinahe-Sicherheitsvorfall“** ein Ereignis mit dem Potenzial, einen Sicherheitsvorfall herbeizuführen, dessen Eintritt aber noch rechtzeitig verhindert werden konnte oder der aus sonstigen Gründen nicht eingetreten ist.

**„kritische Einrichtung“** eine öffentliche oder private Einrichtung, die in Anwendung des § 11 RKEG vom Bundesminister für Inneres als solche eingestuft wurde.

**„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.

**„Mitgliedstaat“** jeder Staat, der Vertragspartei des Vertrags über die Europäische Union in der Fassung BGBl. III Nr. 132/2009 ist.

**„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.

**„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.

**„Sicherheitsvorfall“** ein Ereignis, das die Erbringung eines wesentlichen Dienstes erheblich stört oder stören könnte, einschließlich einer Beeinträchtigung der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit.

**„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-RL angeführten Kategorien in den gelisteten Sektoren und Teilsektoren erbracht werden.

**„Drittstaat“** jeder Staat, der nicht Vertragspartei des Vertrags über die Europäische Union in der Fassung BGBl. III Nr. 132/2009 ist.

# 3 Risikoanalyse

Die Risikoanalyse<sup>7</sup> gemäß § 10 RKEG bildet das analytische Fundament dieser Strategie. Sie dient der systematischen Erfassung, Bewertung und Priorisierung von Gefahren, Schwachstellen und Abhängigkeiten, deren Eintritt oder Wechselwirkung die Aufrechterhaltung wesentlicher gesellschaftlicher und wirtschaftlicher Funktionen gefährden könnte.

Verantwortlich für die Durchführung der Risikoanalyse ist der Bundesminister für Inneres, der den fachlich zuständigen Bundesministerien, den Ländern und den betroffenen Interessenvertretungen Gelegenheit zur Äußerung gibt (§ 10 Abs. 1 RKEG). Damit wird ein sektorübergreifender, kooperativer Prozess etabliert, der alle relevanten Akteure des nationalen Sicherheits- und Krisenmanagements einbindet.

Das methodische Vorgehen orientiert sich an den international anerkannten Grundsätzen des Risikomanagements nach ISO 31000:2018<sup>8</sup> sowie an der ÖNORM-Reihe D 4900<sup>9</sup>, welche den Stand der Technik für einheitliche und nachvollziehbare Risikoanalysen in Österreich festlegen. Diese Standards konkretisieren die gesetzlichen Anforderungen und gewährleisten, dass die Risikoanalyse nicht als einmalige Datenerhebung, sondern als fortlaufender, lernorientierter Prozess verstanden wird. Gleichzeitig erfüllen diese Standards die Vorgaben der RKE-Richtlinie, die die Mitgliedstaaten verpflichtet, regelmäßig nationale Risikoanalysen durchzuführen und die Ergebnisse in ihre Strategien einzubeziehen.

## 3.1 Festlegung des Kontexts

Am Beginn jeder Risikoanalyse steht die Festlegung des Kontexts, in dem Risiken entstehen und bewertet werden. Diese Phase schafft das begriffliche und organisatorische Fundament für den gesamten Prozess.

---

<sup>7</sup> BMI (2026).

<sup>8</sup> ISO (2018).

<sup>9</sup> Austrian Standards International (2021).

Dabei wird zunächst der externe Kontext definiert, also jenes politische, rechtliche, wirtschaftliche, technologische und gesellschaftliche Umfeld, das die Stabilität und Verwundbarkeit kritischer Einrichtungen beeinflusst. Dazu zählen Verpflichtungen hinsichtlich Vorgaben der EU, nationale Strategien wie die Österreichische Sicherheitsstrategie 2024 oder sektorale und regionale Besonderheiten.

Ergänzend wird der interne Kontext erhoben, der die Strukturen, Zuständigkeiten und Prozesse innerhalb der betroffenen Behörden und kritischen Einrichtungen beschreibt. Hier werden bestehende Schutzmaßnahmen, organisatorische Resilienzmechanismen und Kommunikationswege erfasst, um die Fähigkeit zur Krisenbewältigung realistisch einschätzen zu können.

Ein dritter Bestandteil dieser Phase ist die Analyse von Schnittstellen und Abhängigkeiten. § 10 Abs. 2 Z 3 RKEG verpflichtet ausdrücklich zur Berücksichtigung grenzüberschreitender und sektorübergreifender Interdependenzen, etwa zwischen den Sektoren Energieversorgung und Gesundheit. Beispielsweise kann die dauerhafte flächendeckende Gesundheitsversorgung nicht gewährleistet werden, wenn der Energiebedarf als Grundvoraussetzung nicht abgedeckt wird.

Die Risikoanalyse berücksichtigt auch sogenannte „Low Probability/High Impact Risks“. Dabei handelt es sich um Ereignisse mit geringer Wahrscheinlichkeit, deren Auswirkungen jedoch schwerwiegend sein können.

Darüber hinaus behandelt die Risikoanalyse sogenannte „Emerging Risks“, noch nicht vollständig verstandene Risiken. Diese stellen eine Herausforderung dar, da es oft keine historischen Daten zur Bewertung gibt und traditionelle Methoden nur eingeschränkt anwendbar sind.<sup>10</sup> Darunter kann es sich beispielsweise um neuartige Cyber-Bedrohungen, technologisch bedingte Systeminterdependenzen sowie unvorhersehbare Störungen in globalen Versorgungsketten, ebenso wie Entwicklungen im Bereich künstlicher Intelligenz, digitaler Abhängigkeiten, komplexer Lieferketten, neuer Infektionskrankheiten, Einschleppung und Ausbreitung von nicht heimischen Tier- und Pflanzenspezies oder technologischer Systemintegration, handeln.

---

<sup>10</sup> Mazri, C. (2017).

## 3.2 Der Risikomanagementprozess

Auf der Grundlage des definierten Kontexts folgt die Durchführung der eigentlichen Risiko-  
beurteilung. Nach ISO 31000 und der ÖNORM D 4900 gliedert sich diese in vier aufeinander  
aufbauende Phasen.

Die Risikoidentifizierung zielt darauf ab, potenzielle Gefahren und Ereignisse zu erkennen,  
die den Betrieb kritischer Einrichtungen beeinträchtigen könnten. Erfasst werden anthro-  
pogene, technische, intentionale Gefahren und Naturgefahren, sowie grenzüberschrei-  
tende und sektorübergreifende Abhängigkeiten. Dabei werden sowohl historische Ereig-  
nisse als auch neue Risikoquellen berücksichtigt, sowie auf die Expertise von Vertreterinnen  
und Vertretern der Sektoren zurückgegriffen, um ein möglichst vollständiges Lagebild zu  
erhalten.

In der anschließenden Risikoanalyse werden die identifizierten Risiken hinsichtlich Eintritts-  
wahrscheinlichkeit und Auswirkung untersucht. Diese Bewertung erfolgt qualitativ oder se-  
miquantitativ und bildet die Grundlage für die Erstellung einer Risikomatrix, die eine ein-  
heitliche Vergleichbarkeit der Ergebnisse sicherstellt.

Die darauffolgende Risikobewertung dient der Priorisierung. Hier werden die Risiken in Be-  
zug auf festgelegte Kriterien, wie etwa Kritikalität, Schadensausmaß oder Wiederherstel-  
lungszeit, eingeordnet. Ziel ist es, jene Risiken zu identifizieren, die im nichtakzeptablen Be-  
reich liegen und bei denen sofortige Maßnahmen erforderlich sind.

Schlussendlich umfasst die Risikobehandlung die Auswahl und Umsetzung geeigneter Maß-  
nahmen zur Risikominderung. Dies kann technische oder organisatorische Vorkehrungen  
ebenso betreffen, wie die Verlagerung oder Akzeptanz bestimmter Restrisiken.

Dieser gesamte Prozess ist kein einmaliges Verfahren, sondern ein dynamischer Zyklus, in  
dem Erkenntnisse aus der Praxis, neue Bedrohungen oder wissenschaftliche Entwicklungen  
laufend einfließen.

## 3.3 Kommunikation, Überwachung und Aktualisierung

Parallel zu den vier Kernphasen laufen kontinuierliche Prozesse der Kommunikation, Über-  
wachung und Überprüfung. Diese stellen sicher, dass relevante Informationen zwischen

dem Bundesministerium für Inneres, den anderen involvierten Behörden, Ländern, kritischen Einrichtungen und der EU ausgetauscht werden. Die Einbindung unterschiedlicher Akteure fördert Transparenz, stärkt die gemeinsame Risikowahrnehmung und schafft die Grundlage für kohärente Entscheidungen.

Die Risikoanalyse ist regelmäßig zu überprüfen und bei Bedarf zu aktualisieren, insbesondere, wenn sich Gefährdungslagen wesentlich verändern. Dadurch wird gewährleistet, dass die Strategie auf einem aktuellen, wissenschaftlich fundierten Wissensstand basiert und neue Risiken zeitnah berücksichtigt werden. Dieser kontinuierliche Prozess folgt den Grundprinzipien der ISO 31000.

### **3.4 Ergebnisverwendung**

Die Ergebnisse der Risikoanalyse fließen direkt in die Definition der strategischen Leitlinien und Ziele, in die Entwicklung der Maßnahmen zur Stärkung der Resilienz sowie in die Evaluierung und Fortschreibung der Strategie ein. Auf diese Weise bildet die Risikoanalyse den verbindlichen analytischen Kern der gesamten Strategie und gewährleistet, dass alle strategischen Entscheidungen auf überprüfbar, objektiv bewerteten Grundlagen beruhen.

# 4 Strategische Ausrichtung

Die Mission dieser Strategie besteht darin, den nationalen Rahmen für ein systemisch, risikoorientiertes und koordiniertes Resilienzmanagement kritischer Einrichtungen zu schaffen. Sie legt Leitlinien, Ziele, Maßnahmen und Zuständigkeiten fest, die Behörden und kritische Einrichtungen dabei unterstützen, die gesetzlichen Anforderungen des RKEG wirksam umzusetzen und sektorübergreifende, sowie grenzüberschreitende Abhängigkeiten angemessen zu berücksichtigen.

Die Strategie verfolgt die Vision, dass kritische Einrichtungen in Österreich ihre für das Gemeinwesen wesentlichen Dienste auch während Störungen, Krisen und sogar Katastrophen dauerhaft, sicher und verlässlich bereitstellen können. Grundlage ist ein kohärentes, risikobasiertes und europarechtskonformes Resilienzsystem gemäß RKEG und RKE-Richtlinie.

Das Handeln auf Basis dieser Strategie orientiert sich an den Grundsätzen der Rechtmäßigkeit, Verhältnismäßigkeit und Transparenz. Resilienzmaßnahmen werden risikobasiert, evidenzgestützt und unter Nutzung anerkannter Standards des Risikomanagements<sup>11</sup> geplant. Die Zusammenarbeit zwischen Behörden, kritischen Einrichtungen und Interessenvertretungen erfolgt sektorübergreifend und im Einklang mit den unionsrechtlichen Vorgaben. Kontinuierliche Verbesserung und Lernen aus Ereignissen, Übungen und Evaluierungen sind integrale Bestandteile des Resilienzsystems.

Ziel dieser Strategie ist es, einen Rahmen zu schaffen, um die Widerstandsfähigkeit kritischer Einrichtungen in Österreich nachhaltig zu stärken und dadurch die Kontinuität wesentlicher gesellschaftlicher und wirtschaftlicher Funktionen sicherzustellen. Der strategische Ansatz folgt § 9 Abs. 2 Z 1 RKEG, wonach übergeordnete Zielsetzungen festzulegen sind, die die Umsetzung des Gesetzes in kohärente, messbare und überprüfbare Handlungsfelder übersetzen.

Die Resilienz kritischer Einrichtungen wird dabei gemäß § 3 Z 2 RKEG als die folgende Fähigkeit verstanden:

---

<sup>11</sup> ISO 31000 und ÖNORM D 4900-Reihe.

„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.“

## 4.1 Strategische Leitlinien

Diese Strategie basiert auf fünf miteinander verbundenen, wissenschaftlich fundierten<sup>12</sup> Prinzipien:

Erstens verfolgt sie das Prinzip der Vorsorge. Risiken sollen in Zusammenarbeit und im regelmäßigen Austausch mit kritischen Einrichtungen, sowie durch interne Informationsbeschaffung frühzeitig erkannt und auf Grundlage der nationalen Risikoanalyse systematisch adressiert werden.

Zweitens stützt sich die Strategie auf das Prinzip der Kooperation. Da kritische Einrichtungen in wechselseitigen Abhängigkeiten stehen, kann Resilienz nur durch abgestimmtes Handeln in Zusammenarbeit mit dem Bundesminister für Inneres erreicht werden. Betroffene Bundesministerien, sowie Länder, kritische Einrichtungen und Interessenvertretungen sind gleichermaßen gefordert, ihre Informationsflüsse, Entscheidungswege und Ressourcen unter der stetigen und größtmöglichen Berücksichtigung des Schutzes sensibler Informationen der kritischen Einrichtungen zu koordinieren.

Drittens gilt das Prinzip der Verhältnismäßigkeit. Maßnahmen zur Stärkung der Resilienz müssen angemessen, realistisch und wirksam sein, ohne unverhältnismäßige Belastungen für kritische Einrichtungen zu erzeugen. Dieses Prinzip gewährleistet eine ausgewogene Balance zwischen Sicherheit, Wirtschaftlichkeit und gesellschaftlicher Akzeptanz.

Viertens betont die Strategie das Prinzip der Adaptivität. Resiliente Systeme müssen sich an veränderte Bedrohungen, Technologien und gesellschaftliche Rahmenbedingungen anpassen können. Damit folgt Österreich dem international etablierten Verständnis dynamischer

---

<sup>12</sup> OECD (2025).

Resilienz, wonach Lernfähigkeit und Anpassungsvermögen zentrale Indikatoren der Sicherheitskultur sind.<sup>13</sup>

Fünftens wird das Prinzip der Integration verankert. Physische und digitale Schutzkonzepte werden nicht getrennt betrachtet, sondern in einem gemeinsamen Governance-Rahmen zusammengeführt. Die Verbindung zwischen dieser Strategie und den Zielen der NIS-2-Umsetzung schafft eine integrierte Sicherheitsarchitektur, die auf Kohärenz statt Parallelstrukturen setzt.

Diese fünf Leitlinien bilden den normativen Kern der österreichischen Resilienzpolitik. Sie schaffen den Rahmen, in dem konkrete Ziele, Maßnahmen und Evaluierungsmechanismen entwickelt werden.

## 4.2 Strategische Ziele

Die aus diesen Leitlinien abgeleiteten strategischen Ziele sind rechtlich mit dem RKEG verknüpft.

Das erste Ziel besteht in der Stärkung der sektorübergreifenden Widerstandsfähigkeit kritischer Einrichtungen. Österreich strebt ein konsistentes Resilienzniveau in allen relevanten Sektoren an, wobei Synergien zwischen den Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinфраstruktur, Gesundheit, Trinkwasser, Abwasser, digitaler Infrastruktur, öffentlicher Verwaltung, Weltraum sowie Produktion, Verarbeitung und Vertrieb von Lebensmitteln genutzt werden sollen. Die Grundlage dafür bildet die nationale Risikoanalyse, deren Ergebnisse direkt in sektorspezifische Maßnahmen überführt werden.

Das zweite Ziel betrifft die Erhöhung der Transparenz und Steuerbarkeit von Abhängigkeiten. Durch die Identifikation grenzüberschreitender und sektorübergreifender Interdependenzen sollen Verwundbarkeiten frühzeitig erkannt und geeignete Steuerungsmechanismen etabliert werden. Damit trägt Österreich zur Umsetzung der europäischen Verpflichtung, systemische Risiken in kritischen Infrastrukturen zu minimieren, bei.

---

<sup>13</sup> OECD (2025).

Das dritte Ziel richtet sich auf die Förderung öffentlicher und privater Kooperationen. Informationsaustausch, Risikoanalysen und abgestimmte Übungen werden als zentrale Elemente einer lernenden Sicherheitskultur etabliert. Dieses Ziel folgt der Erkenntnis, dass Resilienz vor allem dort entsteht, wo Vertrauen, Kommunikation und gemeinsames Handeln institutionell verankert sind.<sup>14</sup>

Das vierte Ziel beinhaltet die Integration physischer und cyberbezogener Schutzmaßnahmen. Durch die Verbindung beider Dimensionen wird der Grundsatz der ganzheitlichen Sicherheit umgesetzt. Dies entspricht dem Paradigma „Security by Design“, das in internationalen Best-Practice-Modellen zunehmend als Maßstab für kritische Infrastrukturen gilt.<sup>15</sup>

Das fünfte Ziel betrifft die Unterstützung der kritischen Einrichtungen. Der Bundesminister für Inneres verpflichtet sich kritische Einrichtungen beim Ergreifen von Resilienzmaßnahmen zu unterstützen und darüber hinaus unter bestimmten Voraussetzungen auch Frühwarnungen und sektorspezifische Informationen an die kritischen Einrichtungen zu übermitteln. Ebenfalls ist geplant, Beratungen und Schulungen für das Personal kritischer Einrichtungen durchzuführen, sowie Muster und Vorlagen für Risikoanalysen und Resilienzpläne bereitzustellen.

Jedes dieser Ziele ist darauf ausgerichtet den Schutzgrad kritischer Einrichtungen zu erhöhen, die Kontinuität wesentlicher Dienste zu sichern und die Fähigkeit des Staates zu stärken, Krisen vorzubeugen, ihnen standzuhalten und sich davon rasch zu erholen.

---

<sup>14</sup> Bryson, J. (2018).

<sup>15</sup> Strauß, S. / Krieger-Lamina, J. (2017).

# 5 Steuerungs- und Koordinationsrahmen

Der Erfolg dieser Strategie hängt maßgeblich von einer klaren und rechtskonformen Steuerungs- und Koordinationsstruktur ab. Gemäß § 4 RKEG ist der Bundesminister für Inneres die für die Umsetzung und Weiterentwicklung dieser Strategie zuständige Behörde. Ihm obliegt die übergeordnete Steuerung, die Abstimmung mit anderen Behörden und die Sicherstellung des Informationsaustauschs auf nationaler und europäischer Ebene sowie die Zusammenarbeit mit Drittstaaten.

## 5.1 Steuerung und Koordination

Das RKEG verpflichtet Verfahren zur Steuerung und Koordination der Umsetzung der Strategie festzulegen. Diese Verfahren werden durch den Bundesminister für Inneres bestimmt und gewährleisten, dass die im Gesetz vorgesehenen Aufgaben einheitlich und nachvollziehbar wahrgenommen werden.

Die Koordination umfasst insbesondere die Abstimmung der in dieser Strategie vorgesehenen Maßnahmen, die Evaluierung ihrer Wirksamkeit, sowie die Verbindung mit der Risikoanalyse nach § 10 RKEG und der Ermittlung kritischer Einrichtungen nach § 11 RKEG.

Damit wird eine fortlaufende Kohärenz zwischen Risikoanalyse, strategischen Zielen und Umsetzungsmaßnahmen sichergestellt. Die organisatorische Ausgestaltung der Koordination liegt im Verantwortungsbereich des Bundesministers für Inneres und richtet sich nach den bestehenden Verwaltungsstrukturen und rechtlichen Zuständigkeiten.

Der Bundesminister für Inneres sorgt dafür, dass der Informationsaustausch zwischen der RKE-Behörde und dem Bundesamt für Cybersicherheit sichergestellt ist. Diese Koordination dient der Vermeidung von Doppelstrukturen und der Nutzung gemeinsamer Erkenntnisse, soweit dies nach den gesetzlichen Bestimmungen zulässig ist. Darüber hinaus erfolgt der Informationsaustausch mit den zuständigen Stellen der EU. Österreich erfüllt damit die unionsrechtlichen Anforderungen an Transparenz und Berichterstattung gegenüber der Europäischen Kommission.

## 5.2 Identifikation kritischer Einrichtungen

Die Identifikation kritischer Einrichtungen bleibt ein eigenständiger, rechtsförmig ausgestalteter Verwaltungsprozess und wird durch diese Strategie nicht inhaltlich näher bestimmt. Die Strategie verweist jedoch auf dessen grundlegende Bedeutung für die Umsetzung der unionsrechtlichen Vorgaben, da die Identifikation kritischer Einrichtungen die Voraussetzung für die Anwendung der strategischen, organisatorischen und operativen Maßnahmen des RKEG bildet.

Das RKEG sieht vor, dass kritische Einrichtungen anhand bestimmter Kriterien per Bescheid ermittelt werden. Zur Festlegung und näheren Definition einer dieser Voraussetzungen, konkret ob ein Sicherheitsvorfall eintreten kann, wird der Bundesminister für Inneres eine entsprechende Verordnung veröffentlichen. Bei dem Verfahren zur Ermittlung als kritische Einrichtung kommt den potentiellen kritischen Einrichtungen eine Mitwirkungspflicht zu. Mit bescheidmäßiger Ermittlung haben die kritischen Einrichtungen die im RKEG festgelegten Aufgaben zu erfüllen. Für diesen Prozess stellt die vorliegende Strategie einen übergeordneten Orientierungsrahmen dar.

## 5.3 Auflistung der betroffenen Behörden, beteiligten Bundesministerien, Länder und Interessenvertretungen

Die zuständige Behörde für die Umsetzung und den Vollzug des RKEG ist der Bundesminister für Inneres. In weiterer Folge sind jedoch weitere Bundesministerien, die Länder und andere Behörden direkt oder indirekt von den Regelungen des RKEG betroffen, da diese Stellen einerseits selbst als kritische Einrichtungen im Sektor öffentliche Verwaltung eingestuft werden können (mit Ausnahme der Länder und einzelner Bundesministerien) und andererseits da sie kritische Einrichtungen in anderen Sektoren betreiben.

Aus diesen Gründen ist es wichtig für die Erstellung dieser Strategie die betroffenen Stellen entsprechend einzubinden, weshalb im Zuge der Erstellung den folgenden Bundesministerinnen und Bundesministern, den Ländern sowie Interessenvertretungen Gelegenheit zur Äußerung gegeben wurde und diese Äußerungen entsprechend eingearbeitet wurden.

Gemäß § 9 Abs. 1 RKEG wurde eine Aufzählung der betroffenen Bundesministerien, Ländern und Interessenvertretungen in einer Liste im Anhang 1 zusammengefasst.

Dem Bundesministerium für Justiz sowie dem Bundesministerium für Landesverteidigung wurde ebenso Gelegenheit zur Äußerung gegeben. Diese beiden Bundesministerien unterliegen nicht den Bestimmungen des RKEG, haben allerdings die notwendigen strukturellen Voraussetzungen zur Sicherstellung eines hohen Resilienzniveaus zu schaffen.

Die Betroffenheit anderer Behörden (außer die des Bundeamtes für Cybersicherheit) kann erst im Anschluss an die Ermittlung als kritische Einrichtung festgestellt werden. Daher konnte im Zuge dieser Strategie den weiteren Behörden keine Gelegenheit zur Äußerung eingeräumt werden. Dies wird im Rahmen der Evaluierung und Anpassung dieser Strategie erfolgen.

## 6 Evaluierung und Anpassung

Die kontinuierliche Überprüfung und Weiterentwicklung der Strategie ist ein gesetzlich verankerter Bestandteil des Resilienzsystems. Das RKEG verpflichtet den Bundesminister für Inneres dazu, die Strategie in regelmäßigen Abständen zu evaluieren und gegebenenfalls anzupassen. Dieser Prozess stellt sicher, dass die strategischen Zielsetzungen und Maßnahmen auch längerfristig wirksam bleiben und sowohl den aktuellen Risikolagen, als auch den organisatorischen, technologischen und unionsrechtlichen Entwicklungen entsprechen.

Die Evaluierung erfolgt längstens nach vier Jahren ab Beschlussfassung dieser Strategie durch die Bundesregierung. Sie umfasst die Prüfung der Wirksamkeit der Ziele der Strategie, einschließlich der Maßnahmen zur Verbesserung der Resilienz, der Einbindung der zuständigen Bundesministerien, Länder und Interessensvertretungen sowie der Unterstützungsstrukturen für kritische Einrichtungen. Grundlage der Evaluierung sind die Umsetzungsstände der Maßnahmen, Erfahrungen der kritischen Einrichtungen, Erkenntnisse aus der Anwendung des, im RKEG vorgesehenen, Verfahrens zur Ermittlung kritischer Einrichtungen sowie die Ergebnisse der Risikoanalyse.

Im Zentrum der Evaluierung steht die Frage, ob die Ziele der Strategie erreicht werden und ob die gesetzten Maßnahmen geeignet sind, die Resilienz kritischer Einrichtungen nachhaltig zu erhöhen. Die Bewertung orientiert sich an etablierten Modellen der strategischen Steuerung im öffentlichen Sektor. Dazu gehören insbesondere die Analyse des Umsetzungsfortschritts, die Wirkung der Koordinationsmechanismen sowie die Frage, ob neue Risiken, Bedrohungen oder Abhängigkeiten eine Anpassung erforderlich machen.<sup>16</sup>

Die Ergebnisse dieser Evaluierung bilden die Grundlage für eine allfällige Fortschreibung der Strategie. Eine Anpassung ist insbesondere dann erforderlich, wenn sich Änderungen in der Risikolandschaft ergeben, wenn unionsrechtliche Vorgaben aktualisiert werden oder wenn sich aus realen Störungsereignissen oder Übungen neue Erfahrungen ableiten lassen, spätestens jedoch alle vier Jahre.

---

<sup>16</sup> Bovaird, T. / Löffler, E. (2009); Gourmelon, A. / Mroß, M. / Seidel, S. (2011).

Zur Sicherstellung eines nachvollziehbaren und wirksamen Evaluierungsprozesses werden die Ergebnisse dokumentiert. Soweit gesetzlich zulässig und keine Interessen des Bundesministeriums für Inneres dagegensprechen, können wesentliche Erkenntnisse öffentlich zugänglich gemacht werden, um Transparenz zu gewährleisten und die Akzeptanz der strategischen Weiterentwicklung zu stärken. Bestehen unionsrechtliche Berichtspflichten im Zusammenhang mit der Resilienz kritischer Einrichtungen, werden diese in den Fortschreibungsprozess integriert, sodass nationale und europäische Anforderungen aufeinander abgestimmt bleiben.

Die Evaluierung und Anpassung der Strategie bildet somit einen zyklischen Prozess, der sicherstellt, dass die Maßnahmen zur Verbesserung der Resilienz wirksam und aktuell sind. Dieser Ansatz entspricht sowohl den gesetzlichen Vorgaben des RKEG, als auch den wissenschaftlichen Erkenntnissen zur strategischen Governance- und Resilienzentwicklung, die betonen, dass lernfähige und adaptive Strategien besonders wirkungsvoll sind.<sup>17</sup>

---

<sup>17</sup> Gourmelon, A. / Mroß, M. / Seidel, S. (2011).

# 7 Maßnahmen zur Verbesserung der Resilienz kritischer Einrichtungen

Die vorliegende Strategie legt die Grundsätze und Prioritäten der Maßnahmen dar, die zur Verbesserung der Resilienz kritischer Einrichtungen in Österreich erforderlich sind. Diese Maßnahmen beruhen unter anderem auf der Analyse des nationalen Risikoumfelds. Die Strategie definiert keine operativen Detailmaßnahmen, sondern den übergeordneten Rahmen, innerhalb dessen die kritischen Einrichtungen, zuständigen Behörden und relevanten Akteure ihre gesetzlichen Verpflichtungen erfüllen.

## 7.1 Grundsätze der Maßnahmenplanung

Die Maßnahmen zur Verbesserung der Resilienz kritischer Einrichtungen orientieren sich an Grundsätzen, die sich aus dem RKEG sowie aus den einschlägigen internationalen Normen und wissenschaftlichen Erkenntnissen ergeben. Maßnahmen können nur im Rahmen der budgetären Möglichkeiten gesetzt werden.

Alle Maßnahmen müssen im Einklang mit den Bestimmungen des RKEG, sowie den einschlägigen unionsrechtlichen Vorgaben stehen. Die Verhältnismäßigkeit ergibt sich aus der Risikobewertung. Maßnahmen müssen auf den Ergebnissen der Risikoanalyse und der Identifikation kritischer Einrichtungen beruhen. Im Sinne des RKEG und der Resilienzforschung liegen Prävention und Vorbereitung im Vordergrund, da sie die Wirksamkeit nachgelagerter Reaktionen wesentlich erhöhen.<sup>18</sup> Da gemäß § 10 Abs. 2 Z 3 RKEG sektorübergreifende Abhängigkeiten wesentliche Risikofaktoren darstellen, müssen Maßnahmen in allen Sektoren konsistent gestaltet werden, um Wechselwirkungen angemessen zu berücksichtigen.

---

<sup>18</sup> Fekete, A. (2024).

## 7.2 Maßnahmenkategorien

Das RKEG gibt keine spezifischen Einzelmaßnahmen vor, erlaubt aber die Festlegung strategischer Maßnahmenkategorien. Diese Kategorien spiegeln den Stand der Wissenschaft wider und sind mit den gesetzlichen Vorgaben vereinbar. Sie bilden den Leitfaden, innerhalb dem die kritischen Einrichtungen ihre individuellen Verpflichtungen erfüllen.

Organisatorische Maßnahmen umfassen Strukturen, Verfahren und Zuständigkeiten, die notwendig sind, um Resilienzprozesse dauerhaft zu verankern. Dazu zählen insbesondere, Etablierung risikoorientierter Managementprozesse, klare Zuordnung von Verantwortlichkeiten, interne Kommunikations- und Meldewege sowie Notfallvorsorge- und Kontinuitätsprozesse. Solche Maßnahmen entsprechen internationalen Standards zur Resilienzplanung im öffentlichen und privaten Sektor.<sup>19</sup>

Technische und infrastrukturelle Maßnahmen betreffen beispielsweise bauliche, technische oder digitale Schutzmechanismen, die zur Verringerung von Störungsrisiken beitragen. Die Risikoanalyse identifiziert technische Gefahren, die insbesondere robuste Infrastrukturen und redundante Systeme erfordern. Die Maßnahmen sind risikoadaptiert auszugestalten und orientieren sich an anerkannten Normen, wie etwa die ÖNORM D 4900 Reihe.

Maßnahmen zur Stärkung der betrieblichen Resilienz umfassen insbesondere die Personalqualifikation und Schulung, regelmäßige Übungen, organisatorische Lernprozesse sowie vorausschauende Planung und Szenarienanalysen.

Im Rahmen von kooperativen und koordinativen Maßnahmen identifiziert die Risikoanalyse sektorübergreifende und grenzüberschreitende Abhängigkeiten. Maßnahmen zur Resilienzsteigerung in diesem Bereich erfordern daher den Austausch zwischen kritischen Einrichtungen, die Abstimmung mit zuständigen Behörden, Bundesministerien und Ländern, die sektorübergreifende Zusammenarbeit mit kritischen Einrichtungen und schlussendlich die internationalen Kooperationen mit europäischen Mitgliedstaaten und Drittstaaten.

Präventive und reaktive Maßnahmen im Umgang mit intentionalen Gefahren um absichtliche Störungen kritischer Einrichtungen hintanzuhalten, erfordern Unterstützungs- und Schutzmaßnahmen, die im Rahmen der gesetzlichen Möglichkeiten mit Sicherheitsbehörden

---

<sup>19</sup> Haubner, O. / Pröhl, M. / Proeller, I. / Rieder, S. / von Natzmer, W. / Fieseler, J. (2006).

den abgestimmt werden müssen. Die Maßnahmen orientieren sich an Risikoanalysen (seitens der Republik und der kritischen Einrichtungen) zu intentionalen Gefahren und den Erkenntnissen der Sicherheitsforschung.<sup>20</sup>

### 7.3 Unterstützung kleiner und mittlerer Unternehmen

Gemäß RKEG werden die Unterstützungsmaßnahmen zur Umsetzung von Verpflichtungen für kleine und mittlere Unternehmen beschrieben. Diese Unterstützung wird im Rahmen der gesetzlichen Vorgaben erfolgen und wird die Bereitstellung von Orientierungshilfen und Leitfäden, Informations- und Beratungsmöglichkeiten, sektorspezifische Austauschformate sowie Schulungen und Awareness-Maßnahmen umfassen. Diese Unterstützungsformen sollen die Resilienz kleiner und mittlerer Unternehmen stärken, ohne deren Eigenverantwortung einzuschränken.

Laufend findet intensiver Austausch mit Interessenvertretungen statt. Dies soll einen guten Informationsfluss an die voraussichtlich betroffenen kleinen und mittleren Unternehmen sicherstellen.

### 7.4 Zusammenhang Gefahrenkategorien und mögliche Maßnahmen

Um auf die Kategorien des Gefahrenkatalogs der Risikoanalyse entsprechend reagieren zu können, können kritische Einrichtungen beispielsweise folgende Maßnahmen treffen:

- Naturgefahren ⇒ technische und bauliche Maßnahmen
- technische Gefahren ⇒ technische Maßnahmen
- anthropogene Gefahren ⇒ technische und organisatorische Maßnahmen
- intentionale Gefahren ⇒ technische, organisatorische und personelle Maßnahmen (gegebenenfalls in Kooperation mit Sicherheitsbehörden)
- sektorübergreifende Abhängigkeiten ⇒ koordinative Maßnahmen
- grenzüberschreitende Abhängigkeiten ⇒ internationale Kooperation

---

<sup>20</sup>Thoma, K. (2014), Max, M. (2024).

Diese Liste beinhaltet eine demonstrative Aufzählung verschiedenster Maßnahmenkategorien, um auf die Gefahrenkategorien des Gefahrenkatalogs der Risikoanalyse reagieren zu können.

# 8 Koordination und Zusammenarbeit mit dem Bundesamt für Cybersicherheit und die europäische Einbettung

Die Erhöhung der Resilienz kritischer Einrichtungen erfordert eine enge und strukturierte Zusammenarbeit sowohl mit dem Bundesamt für Cybersicherheit, als auch mit zuständigen Stellen der EU. Die Strategie muss eine Auflistung der betroffenen Behörden und insbesondere der an der Umsetzung der Strategie beteiligten Bundesministerien, Länder sowie Interessenvertretungen beinhalten, welche in Anhang 1 ersichtlich ist.

Die nationale Strategie steht in engem Zusammenhang mit anderen strategischen und regulatorischen Instrumenten des Bundes. § 9 Abs. 2 Z 7 RKEG verlangt ausdrücklich, dass diese Beziehungen sichtbar gemacht werden. Darüber hinaus besteht eine wesentliche Schnittstelle zur NIS-2-RL und der korrespondierenden nationalen Umsetzung im NISG 2026, da kritische Einrichtungen nach dem RKE-Regime gleichzeitig als wesentliche Einrichtung im Sinne des NIS-2-Regimes gelten.

Um die Resilienz und ein hohes gemeinsames Cybersicherheitsniveau kritischer Einrichtungen gleichermaßen sicherzustellen, ist eine verstärkte Zusammenarbeit zwischen der RKE-Behörde und dem Bundesamt für Cybersicherheit, von besonderer Relevanz.

Das RKEG sieht vor, dass die RKE-Behörde dem Bundesamt für Cybersicherheit die Identität der kritischen Einrichtungen, einschließlich des Sektors und des Teilsektors, in dem diese ihren wesentlichen Dienst erbringen, mitzuteilen hat. Zudem ist in der NIS-2-Richtlinie ebenso vorgesehen, dass eine Zusammenarbeit und ein Informationsaustausch zwischen den beiden Behörden zur Identifizierung von kritischen Einrichtungen stattfinden soll.

Im Allgemeinen umfasst die Zusammenarbeit den regelmäßigen Informationsaustausch über Cybersicherheitsrisiken, Cyberbedrohungen, Beinahe-Cybersicherheitsvorfälle, Cybersicherheitsvorfälle, nicht cyberbezogene Risiken, Bedrohungen, Beinahe-Sicherheitsvorfälle, Sicherheitsvorfälle und die ergriffenen Maßnahmen.

Bei der Ergreifung von Aufsichts- und Durchsetzungsmaßnahmen unterrichtet die RKE-Behörde das Bundesamt für Cybersicherheit über die getroffenen Maßnahmen und die Ergebnisse der Überprüfungen. Dieser Mechanismus ist spiegelbildlich ebenso in der NIS-2-Richtlinie vorgesehen.

Die oben angeführten Verpflichtungen der Behörden tragen unter dem Blickwinkel der verzahnten Umsetzung und der Bereitstellung von umfangreichen Information zu einer Erhöhung der Resilienz bei.

Da Sicherheitsvorfälle meist physische und cyberbezogene Komponenten aufweisen, ist geplant, dass der künftige Meldeprozess aller Akteure nach dem RKEG und der NIS-2-Richtlinie in einer koordinierten technischen Lösung erfolgt. Der Vorteil eines koordinierten Meldeprozesses besteht für meldepflichtige Einrichtung in der Möglichkeit, dass die Meldung beiden zuständigen Behörden gleichermaßen zugehen kann. Dies erspart doppelte Prozesswege und wertvolle Zeit in herausfordernden Situationen, wie bei der Behandlung von Sicherheitsvorfällen. Bei Nachmeldungen kann auf diese Weise der Bearbeitungsaufwand begrenzt werden. Aus behördlicher Sicht wird durch eine koordinierte technische Lösung der Verwaltungsaufwand erheblich minimiert.

Durch diesen strukturierten und rechtssicher ausgestalteten Koordinierungsrahmen wird gewährleistet, dass die Strategie konsistent bleibt, die gesetzlichen Anforderungen erfüllt und mit den nationalen sowie europäischen Zielsetzungen harmonisiert. Die enge Verzahnung mit relevanten Behörden, Interessenvertretungen und unionsrechtlichen Instrumenten stellt sicher, dass Resilienzpolitik in Österreich kohärent, adaptiv und langfristig wirksam ausgestaltet wird.

## 9 Ausblick

Die Umsetzung dieser Strategie bildet den Ausgangspunkt für einen kontinuierlichen Verbesserungsprozess unter Orientierung an den einschlägigen Standards des Risikomanagements. Die kommenden Jahre bieten die Chance, sektorübergreifende Kooperationen zu vertiefen, den Informationsaustausch zu optimieren und weitere Harmonisierungen mit unionsrechtlichen Vorgaben weiter auszubauen, sowie Erfahrungswerte zu nutzen. Fortschritte in Digitalisierung, Datengrundlagen und Analyseverfahren können die Qualität der Risikoanalyse gemäß § 10 RKEG steigern und dadurch die Wirksamkeit der Maßnahmen verbessern. Die fortlaufende Evaluierung bildet dabei die Grundlage für eine adaptive, lernorientierte und evidenzbasierte Weiterentwicklung des nationalen Resiliensystems der Republik Österreich.

# Quellen- & Literaturverzeichnis

**Austrian Standards International:** ÖNORM D 4900:2021-01. Risikomanagement für Organisationen und Systeme – Begriffe und Grundlagen – Anleitung zur Umsetzung der ISO 31000. Wien: Austrian Standards 2021a.

**Austrian Standards International:** ÖNORM D 4901:2021-01. Risikomanagement für Organisationen und Systeme – Anforderungen an das Risikomanagementsystem – Anleitung zur Umsetzung der ISO 31000. Wien: Austrian Standards 2021a.

**Austrian Standards International:** ÖNORM D 4902-1:2021-01. Risikomanagement für Organisationen und Systeme – Leitfaden – Teil 1: Einbettung des Risikomanagements ins Managementsystem – Anleitung zur Umsetzung der ISO 31000. Wien: Austrian Standards 2021b.

**Austrian Standards International:** ÖNORM D 4902-2:2021-01. Risikomanagement für zur Organisationen und Systeme – Leitfaden – Teil 2: Methoden der Risikobeurteilung – Anleitung Umsetzung der ISO 31000. Wien: Austrian Standards 2021c.

**Austrian Standards International:** ÖNORM D 4902-3:2021-01. Risikomanagement für Organisationen und Systeme – Leitfaden – Teil 3: Notfall-, Krisen- und Kontinuitätsmanagement – Anleitung zur Umsetzung der ISO 31000. Wien: Austrian Standards 2021d.

**Austrian Standards International:** ÖNORM D 4903:2021-01. Risikomanagement für Organisationen und Systeme – Anforderungen an die Qualifikation des Risikomanagers – Anleitung zur Umsetzung der ISO 31000. Wien: Austrian Standards 2021e.

**BKA - Bundeskanzleramt:** Österreichische Sicherheitsstrategie 2024. Wien 2024.  
<https://www.bundeskanzleramt.gv.at/themen/sicherheitspolitik/sicherheitsstrategie.html>.

**BKA - Bundeskanzleramt/BMI - Bundesministerium für Inneres:** Österreichisches Programm zum Schutz kritischer Infrastrukturen (APCIP) Masterplan 2014. Wien 2015.  
[Österreichisches Programm zum Schutz kritischer Infrastrukturen \(APCIP\)](#).

**BKA - Bundeskanzleramt/BMI - Bundesministerium für Inneres:** Österreichische Cyber-Sicherheitsstrategie 2021. Wien 2021.

<https://www.bundeskanzleramt.gv.at/themen/cybersicherheit/oesterreichische-strategie-fuer-cybersicherheit.html>.

**BMI - Bundesministerium für Inneres:** Nationale Risikoanalyse gem. RKEG. Wien 2026.

**Boin, A./Lodge, M.:** Designing Resilient Institutions for Transboundary Crisis Management: A Time for Public Administration. In: McDonald, Bruce D. (Hg.): Public Administration, Hoboken: John Wiley & Sons 2016.

**Boin, A./McConnell, A.:** Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience. In: Coombs, W. Timothy (Hg.): Journal of Contingencies and Crisis Management, Oxford/Malden: Blackwell Publishing 2007.

**Bovaird, T./Löffler, E.:** Public Management and Governance. London/New York: Routledge 2009.

**Bryson, John M.:** Strategic Planning for Public and Nonprofit Organizations: A Guide to Strengthening and Sustaining Organizational Achievement. Hoboken: Wiley & Sons 2018.

**Fekete, A.:** Risiko, Katastrophen und Resilienz - Eine Einführung in Methoden, Konzepte und Themen. Berlin/Heidelberg: Springer 2024.

**Gourmelon, A./Mroß, M./Seidel, S.:** Management im öffentlichen Sektor: Organisationen steuern - Strukturen schaffen - Prozesse gestalten. Heidelberg: Rehm 2011.

**Haubner, O./Pröhl, M./Proeller, I./Rieder, S./von Natzmer, W./Fieseler, J.:** Strategische Steuerung. Dokumentation eines Expertendialoges im Rahmen der Projektinitiative „Staat der Zukunft“. Gütersloh: Bertelsmann Stiftung 2006.

**Hillmann, J./Guenther, E.:** Organizational Resilience: A Review and Synthesis of the Literature. In: Alegre, J./Malik, A./Beauregard, A. (Hg.): International Journal of Management Reviews. London/Hoboken: John Wiley & Sons and the British Academy of Management 2020.

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

**Linkov, I./Trump, B. D.:** The Science and Practice of Resilience. Cham: Springer International Publishing 2019.

**Linkov, I./Eisenberg, D. A./Plourde, K./Seager, T. P./Allen, J. H./Kott, A.:** Resilience Metrics for Cyber Systems. In: Linkov, I./ Lambert, J. (Hg.): Environment Systems and Decisions, New York: Springer 2013.

**Max, M.:** Resiliente Infrastrukturen - Perspektiven und Handlungsempfehlungen für ein vernetztes Resilienzmanagement. Berlin: Erich Schmidt Verlag 2024.

**Mazri, C.:** (Re)Defining Emerging Risks. In: Cox, A. (Hg.): Risk Analysis. Hoboken: Wiley Blackwell 2017.

**OECD:** Building Anticipatory Capacity with Strategic Foresight in Government: Lessons from Lithuania, Italy, and Malta. Paris: OECD Publishing 2025.

**Strauß, S./Krieger-Lamina, J.:** Digitaler Stillstand: Die Verletzlichkeit der digital vernetzten Gesellschaft – Kritische Infrastrukturen und Systemperspektiven. Wien: Institut für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften 2017.

**Thoma, K.:** Resilien-Tech: „Resilience-by-Design“: Strategie für die technologischen Zukunftsthemen. Freiburg: acatech – Deutsche Akademie der Technikwissenschaften, 2014.

# Abkürzungsverzeichnis

Abl.	Amtsblatt der Europäischen Union
Abs.	Absatz
Art.	Artikel
BGBI.	Bundesgesetzblatt
EU	Europäische Union
ISO	International Organization for Standardization
KMU	Kleine und mittlere Unternehmen
Nr.	Nummer
OECD	Organisation for Economic Cooperation and Development
ÖNORM	Österreichische Normen
RKEG	Resilienz kritischer Einrichtungen-Gesetz
usw.	und so weiter
Z	Ziffer

# Anhang 1: Liste der an der Strategie beteiligten Stellen

- Bundeskanzleramt
- Bundesministerium für Wohnen, Kunst, Kultur, Medien und Sport
- Bundesministerium für europäische und internationale Angelegenheiten
- Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz
- Bundesministerium für Bildung
- Bundesministerium für Finanzen
- Bundesministerium für Frauen, Wissenschaft und Forschung
- Bundesministerium für Innovation, Mobilität und Infrastruktur
- Bundesministerium für Land- und Forstwirtschaft, Klima- und Umweltschutz, Regionen und Wasserwirtschaft
- Bundesministerium für Wirtschaft, Energie und Tourismus
- Bundesamt für Cybersicherheit
- Land Wien
- Land Niederösterreich
- Land Oberösterreich
- Land Salzburg
- Land Steiermark
- Land Kärnten
- Land Tirol
- Land Vorarlberg
- Land Burgenland
- Wirtschaftskammer Österreich
- Industriellenvereinigung