KIRAS Sicherheitsforschung

Bundesministerium Finanzen

FFG Forschung wirkt.

Leitfäden kritische Einrichtungen

§ 15 Abs. 2 Z 1 bis Z 6 RKEG

Ausgabe: Juni 2026

HOCHSCHULE CAMPUS WIEN UNIVERSITY OF APPLIED SCIENCES

Bundesministerium Inneres

Impressum

Medieninhaberin: Hochschule Campus Wien – Verein zur Förderung des Fachhochschul-, Entwicklungs- und Forschungszentrums im Süden Wiens; ZVR-Zahl 625976320, DVR-Nummer: 2111102, Favoritenstraße 226, 1100 Wien.

Redaktionsteam und für den Inhalt verantwortlich:
FH-Prof.in Mag.a Claudia Körmer, Mag. Wolfgang Tomaschitz,
FH-Prof. DI Dr. Martin Langer, Experten und Expertinnen des BMI
Weiters im Projektteam: Mirjam Habisreutinger MA, Kristina Hauer BA,
Dr.in Beatrice Preßl, Mag. Josef Ruh, David Reiter BSc, Markus Glanzer MBA
Grafik: Doris Zemann (www.dggd.at)
Lektorat: Mag.a Verena Brinda (www.verenabrinda.at)
Produktionskoordination: DI (FH) Mag. Thomas Goiser MBA MA

Die Texte und Daten wurden sorgfältig ausgearbeitet; dennoch können wir keine Haftung für die Richtigkeit der Angaben übernehmen.

DOI: https://doi.org/10.34895/hcw.0033

Kontakt für Feedback: sicherheitsmanagement@hcw.ac.at
Wien, Juni 2026

Dieses Projekt wurde von der Hochschule Campus Wien, Fachbereich Risiko- und Sicherheitsmanagement, mit folgenden Konsortialpartnern umgesetzt:

PROTECTUM Solutions DIE KRISENPLANER

Folgende Organisationen und Unternehmen haben als LOI-Partner mitgewirkt:

Austrian Power Grid
ASFINAG
METRO
OMV
Vivatis
Wiener Linien
Wirtschaftskammer Österreich

Zusätzlich dürfen wir uns bei den nachstehenden Organisationen besonders bedanken:

Verbund AG
Wiener Stadtwerke Gruppe

An der Erstellung dieses Leitfadens haben Vertreterinnen und Vertreter aus kritischen Einrichtungen folgender (Teil-)Sektoren ihre Expertise eingebracht:

Energie: Strom, Fernwärme und -kälte, Erdöl, Erdgas
Verkehr: Schienenverkehr, Straßenverkehr, Öffentlicher Verkehr
Gesundheit
Trinkwasser
Abwasser
Digitale Infrastruktur
Öffentliche Verwaltung
Produktion, Verarbeitung und Vertrieb von Lebensmitteln

Für die wertvollen fachlichen Beiträge, die konstruktiven Rückmeldungen und die engagierte Unterstützung möchte sich das Projektteam bei allen Mitwirkenden herzlich bedanken.

Inhalt

Vorwort

BMI / Pachauer

Sylvia Mayer
Direktorin der DSN

Sehr geehrte Leserinnen und Leser,

die Versorgung mit Energie, Trinkwasser, Gesundheitsleistungen, digitalen Diensten, Verkehrsinfrastruktur oder öffentlichen Verwaltungsleistungen bildet das Fundament unseres gesellschaftlichen und wirtschaftlichen Zusammenlebens. Die zunehmende Vernetzung dieser Systeme, globale Krisenentwicklungen, Naturereignisse, hybride Bedrohungen sowie Cyberangriffe verdeutlichen jedoch, dass die Widerstandsfähigkeit kritischer Einrichtungen heute eine zentrale sicherheits- und wirtschaftspolitische Herausforderung darstellt.

Aus Sicht des Verfassungsschutzes stellen dabei insbesondere extremistische und nachrichtendienstliche Aktivitäten eine Bedrohung für die kritische Infrastruktur dar. Die Europäische Union zeigt seit 2006 Bestrebungen, die europäische kritische Infrastruktur besser vor Angriffen zu schützen.

Als 2008 die EU-Richtlinie über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen, der Vorläufer der heute gültigen Richtlinie über die Resilienz kritischer Einrichtungen, beschlossen wurde, erkannte das Bundesministerium für Inneres gemeinsam mit dem Bundeskanzleramt die Chance, mit dieser Richtlinie einhergehend auch die kritische Infrastruktur mit nationaler Relevanz holistisch zu schützen. Daher wurden die Agenden der nationalen Sicherheit um die der wirtschaftlichen Sicherheit in diesem Bereich erweitert, woraus im Jahr 2008 der Beschluss der Bundesregierung folgte, ein Österreichisches Programm zum Schutz der kritischen Infrastruktur umzusetzen, das im Masterplan 2014 mündete (APCIP 2014).

Über die europäischen Vorgaben hinaus, die ausschließlich den Energie- und Verkehrssektor mit Relevanz für mehrere EU-Staaten erfasste, wurden in Österreich wesentliche kritische Infrastrukturen aller Sektoren erfasst. Dies berücksichtigte die sektorenübergreifenden Abhängigkeiten; besonders erwähnenswert ist der bereits im APCIP 2014 gewählte „All-hazards-Ansatz".

Die Anforderung einer Anpassung erhöhte sich deutlich seit dem Beginn des russischen Angriffskriegs gegen die Ukraine im Februar 2022, mit dem einhergehend erhöhte Bedrohungslagen zu Angriffen auf kritische Infrastruktur, ausländischer Informationsbeeinflussung oder geschürten Unsicherheiten in der Versorgungsicherheit spürbar waren. Darüber hinaus wird die globale Lage durch das vermehrte Auftreten von durch den Klimawandel beförderten Naturkatastrophen verschärft. Diese multiplen Krisen wirken sich auf die Daseinsvorsorge und den Wirtschaftsstandort sowohl in Österreich als auch in der EU aus.

Als Reaktion darauf wurde mit dem Resilienz kritischer Einrichtungen-Gesetz (RKEG), das die europäische Richtlinie über die Resilienz kritischer Einrichtungen in österreichisches Recht umsetzt, ein neuer rechtlicher Rahmen geschaffen. Ziel ist es, die Resilienz der kritischen Einrichtungen im Binnenmarkt mithilfe von harmonisierten Mindestverpflichtungen zu verbessern.

Die Österreichische Strategie für die Resilienz kritischer Einrichtungen bildet dabei den nationalen strategischen Rahmen. Dem Bundesministerium für Inneres und der Direktion Staatsschutz und Nachrichtendienst (DSN) kommt bei der Umsetzung des Resilienz kritischer Einrichtungen-Gesetzes eine zentrale Rolle zu. Als zuständige Behörde verantwortet die DSN die nationale Strategie für die Resilienz kritischer Einrichtungen, führt sektorübergreifende Risikoanalysen durch, identifiziert kritische Einrichtungen und begleitet diese bei der Umsetzung. Darüber hinaus fungiert die DSN als nationale Anlaufstelle für die Zusammenarbeit mit den Organen der EU und den zuständigen Behörden anderer Mitgliedsstaaten.

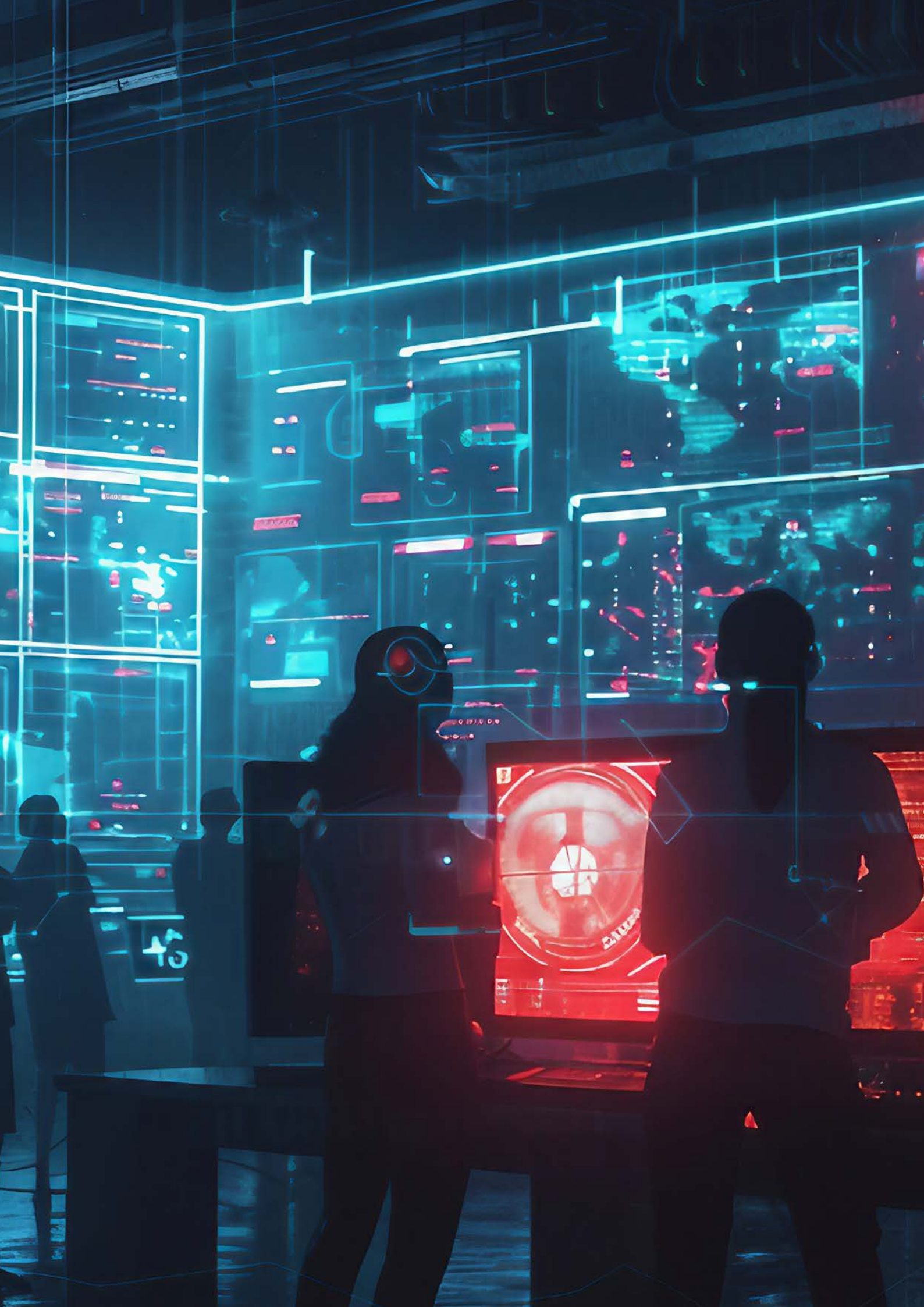
Die Umsetzung der Richtlinie auf nationaler Ebene startete durch die Verabschiedung des Resilienz kritischer Einrichtungen-Gesetzes am 16. Oktober 2025 und die später folgende ergänzende Kundmachung der Resilienz kritischer Einrichtungen-Verordnung. Identifizierte kritische Einrichtungen sind fortan verpflichtet, Sicherheitsvorfälle zu melden, auf Basis der nationalen Risikoanalyse eigene Analysen über die Risikoexposition ihrer kritischen Infrastrukturen durchzuführen und daraus Resilienzmaßnahmen abzuleiten und umzusetzen. Besonders erwähnenswert ist die die für kritische Einrichtungen geltende Meldepflicht von Sicherheitsvorfällen und die Möglichkeit, Beinahe-Sicherheitsvorfälle zu melden. Dies ermöglicht den aktiven Austausch von Informationen zwischen den Behörden und den kritischen Einrichtungen.

Ferner sind Meldungen von Beinahe-Sicherheitsvorfällen im derzeitig zunehmenden Kontext der hybriden Bedrohungen eine wertvolle Möglichkeit für Unternehmen, Anomalien an die Sicherheitsbehörde zu melden. Diese wiederum können aufgrund der analysierten Muster konkretere Handlungsstrategien ableiten.

Im Rahmen ihrer Aufgabenerfüllung kooperiert die DSN intensiv mit österreichischen Forschungseinrichtungen, um den Stand der Wissenschaft in ihre tägliche Arbeit einfließen zu lassen. Diesen Anspruch zeigt auch das von der Hochschule Campus Wien umgesetzte „Projekt zur Unterstützung der kritischen Einrichtungen" (PUKE). Diese kooperative Zusammenarbeit zwischen Behörden, Wissenschaft und Wirtschaft ist Sinnbild für den erfolgreichen Weg, der in Österreich seit 2008 für den Schutz der kritischen Infrastruktur eingeschlagen wurde und seither tägliche Praxis ist.

Die DSN versteht sich bei der Umsetzung des Resilienz kritischer Einrichtungen-Gesetzes als verlässlicher Ansprech- und Kooperationspartner der kritischen Einrichtungen. Ziel ist es, gemeinsam mit den betroffenen Organisationen die Widerstandsfähigkeit wesentlicher Dienstleistungen weiterzuentwickeln und so einen nachhaltigen Beitrag zur Sicherheit und Stabilität Österreichs zu leisten.

Ich bedanke mich im Namen der DSN bei allen, die an der Umsetzung des Resilienz kritischer Einrichtungen-Gesetzes beteiligt waren. In Zeiten volatiler Sicherheitslagen ist Resilienz entscheidend. Eine widerstandsfähige kritische Infrastruktur ist dabei ein Garant für ein sicheres Österreich.



Z 0: Allgemeine Grundlagen und Anwendung des Leitfadens

1 Rechtlicher Rahmen

In einer zunehmend verflochtenen europäischen Wirtschaft kommt kritischen Einrichtungen als Anbietern wesentlicher Dienste eine unverzichtbare Rolle bei der Aufrechterhaltung wichtiger gesellschaftlicher Funktionen und wirtschaftlicher Tätigkeiten zu. Die Richtlinie (EU) 2022/2557 über die Resilienz kritischer Einrichtungen (RKE-Richtlinie) löst die bisherige Richtlinie 2008/114/EG ab und vollzieht einen grundlegenden Paradigmenwechsel: weg vom bloßen Schutz einzelner Infrastrukturobjekte, hin zu einem umfassenden Resilienzansatz, der die Fähigkeit der Einrichtungen zur Aufrechterhaltung ihrer wesentlichen Dienste in den Mittelpunkt stellt. Die RKE-Richtlinie erfasst dabei alle Gefährdungen – natürliche wie von Menschen verursachte, zufällige wie vorsätzliche (All-Gefahren-Ansatz/all-hazards approach).

Die RKE-Richtlinie wurde durch das Resilienz kritischer Einrichtungen-Gesetz (RKEG), BGBl. I Nr. 60/2025, in österreichisches Recht umgesetzt.

In der Folge werden einige wesentliche Begriffe erläutert.

Fokus auf den wesentlichen Dienst
Sämtliche Anforderungen des RKEG (einrichtungsinterne Risikoanalyse, Resilienzmaßnahmen, Meldepflichten, behördliche Aufsicht) sind auf den wesentlichen Dienst der kritischen Einrichtung bezogen. Der wesentliche Dienst ist der alleinige Bezugspunkt des gesamten Regelwerks und somit auch dieser Leitfäden. Die Resilienzmaßnahmen gemäß § 15 RKEG dienen nicht dem allgemeinen Schutz der Einrichtung als Unternehmen, nicht der Absicherung beliebiger Geschäftstätigkeiten und nicht dem umfassenden Schutz aller Vermögenswerte, sondern der Aufrechterhaltung des wesentlichen Dienstes der Einrichtung. Eine Liste wesentlicher Dienste ist in der Delegierten Verordnung (EU) 2023/2450 festgelegt und die Erbringung eines solchen wird für jede kritische Einrichtung im Einstufungsbescheid festgestellt, sofern alle kumulativen Voraussetzungen, um als kritische Einrichtung zu gelten, erfüllt sind.

Die kritische Infrastruktur im Sinne des RKEG umfasst dementsprechend jene „Objekte, Anlagen, Ausrüstungen, Netze, Systeme oder Teile eines Objektes, einer Anlage, einer Ausrüstung, eines Netzes oder eines Systems, die für die Erbringung eines wesentlichen Dienstes erforderlich sind" (§ 3 Z 5 RKEG), nicht die Gesamtheit der Betriebsanlagen der Einrichtung.

Sicherheitsvorfall und Prävention
Ein Sicherheitsvorfall im Sinne des RKEG ist „ein Ereignis, das die Erbringung des wesentlichen Dienstes erheblich stört oder erheblich stören könnte" (§ 3 Z 3 RKEG). Das Merkmal der Erheblichkeit grenzt den Sicherheitsvorfall von alltäglichen betrieblichen Störungen ab. Gegenstand des RKEG sind somit nicht Bagatellstörungen, sondern Ereignisse mit dem Potenzial, die Erbringung des wesentlichen Dienstes substanziell zu beeinträchtigen oder zu unterbrechen.

Die Pflicht zur Verhinderung von Sicherheitsvorfällen (§ 15 Abs. 2 Z 1 RKEG) setzt jedoch nicht erst an der Schwelle der Erheblichkeit an. Prävention bedeutet Ursachen und Wirkungsketten, die zu einem Sicherheitsvorfall führen können, frühzeitig zu erkennen und entsprechende vorbeugende Maßnahmen zu setzen. Das RKEG kennt neben dem Sicherheitsvorfall auch den Beinahe-Sicherheitsvorfall als „ein Ereignis mit dem Potenzial, einen Sicherheitsvorfall hervorzurufen, dessen Eintritt aber noch rechtzeitig verhindert werden konnte oder der aus sonstigen Gründen nicht eingetreten ist" (§ 3 Z 4 RKEG).

Wirksame Prävention erfasst daher auch jene vorgelagerten Zustände, Schwachstellen und Störungen, die – einzeln oder im Zusammenwirken – zu einem Sicherheitsvorfall eskalieren können. Wer ausschließlich auf die Verhinderung bereits erheblicher Störungen abstellt, betreibt keine Prävention, sondern Schadensbegrenzung.

Sektorspezifische Schwellenwerte für meldepflichtige Sicherheitsvorfälle

Die Resilienz kritischer Einrichtungen-Verordnung (RKEV), BGBl. II Nr. 91/2026, konkretisiert die Schwellenwerte für meldepflichtige Sicherheitsvorfälle gemäß § 17 Abs. 1 RKEG. Dabei verwendet die RKEV je nach Sektor und wesentlichem Dienst unterschiedliche Messgrößen. In einer Reihe von Sektoren wird ausschließlich die Dauer des Ausfalls oder der eingeschränkten Verfügbarkeit herangezogen. In anderen Sektoren verwendet die RKEV dagegen kombinierte Messgrößen, die sowohl das Ausmaß als auch die Dauer der Störung abbilden: Nutzerstunden oder Zählpunktstunden. Bei diesen kombinierten Schwellenwerten kann ein kurzer, aber großflächiger Ausfall die Meldeschwelle ebenso überschreiten wie ein lange andauernder, aber lokal begrenzter. Die unterschiedlichen Messgrößen spiegeln die sektorspezifischen Besonderheiten wider und sind für die kritische Einrichtung bei der Planung und Dimensionierung ihrer Resilienzmaßnahmen unmittelbar relevant: Jede Einrichtung muss wissen, welches Kriterium für sie gilt, um ihre einrichtungsinterne Risikoanalyse und Resilienzmaßnahmenplanung daran auszurichten.

Risikoanalyse als Überbau

Das RKEG folgt einer zweistufigen Systematik: Auf Ebene des Bundes führt der Bundesminister für Inneres eine nationale Risikoanalyse gemäß § 10 RKEG durch, die basierend auf dem All-Gefahren-Ansatz zudem sektorübergreifende Abhängigkeiten und die Auswirkungen von Sicherheitsvorfällen auf andere Sektoren berücksichtigt. Die relevanten Elemente dieser nationalen Risikoanalyse werden den kritischen Einrichtungen zur Verfügung gestellt.

Auf Ebene der einzelnen Einrichtung verpflichtet § 14 RKEG jede kritische Einrichtung, auf Grundlage der nationalen Risikoanalyse eine einrichtungsinterne Risikoanalyse durchzuführen und die Ergebnisse strukturiert aufzubereiten. Diese einrichtungsinterne Risikoanalyse hat „die wechselseitige Abhängigkeit zwischen dem von der jeweiligen kritischen Einrichtung erbrachten wesentlichen Dienst und wesentlichen Diensten, die von anderen Einrichtungen der im Anhang der RKE-RL gelisteten Sektoren erbracht werden, zu berücksichtigen" (§ 14 Abs. 2 RKEG). Hat eine kritische Einrichtung aufgrund

anderer rechtlicher Verpflichtungen bereits Risikoanalysen durchgeführt, die hinsichtlich dieser Anforderungen zumindest gleichwertig sind, wird den Anforderungen des § 14 RKEG insoweit entsprochen (§ 14 Abs. 3 RKEG).

§ 14 RKEG bildet damit den Überbau für sämtliche Resilienzmaßnahmen: Die einrichtungsinterne Risikoanalyse liefert die Gesamtbetrachtung der Gefährdungslage, der Abhängigkeiten und der Auswirkungen. § 15 RKEG baut unmittelbar darauf auf und verpflichtet die kritischen Einrichtungen auf Grundlage der Ergebnisse der nationalen Risikoanalyse (gemäß § 10 RKEG) und der einrichtungsspezifischen Risikoanalyse (gemäß § 14 RKEG) „geeignete und verhältnismäßige" Resilienzmaßnahmen zu treffen (§ 15 Abs. 1 RKEG). Die einrichtungsinterne Risikoanalyse bestimmt damit also grundlegend Art, Umfang und Priorisierung der Maßnahmen.

Für die konkrete Ausgestaltung der Maßnahmen nach § 15 Abs. 2 Z 1 bis Z 6 RKEG ist jedoch eine weitergehende, maßnahmenspezifische Risikobetrachtung erforderlich. Während § 14 RKEG die Gefährdungslage der Einrichtung als Ganzes erfasst, verlangt die Umsetzung der einzelnen Resilienzmaßnahmen eine vertiefte Auseinandersetzung mit den jeweils bereichsspezifischen Risiken: etwa den konkreten Bedrohungen für den physischen Schutz (Z 2), den spezifischen Szenarien für Sicherheitsvorfälle und deren Bewältigung (Z 3) oder den für die Betriebskontinuität relevanten Abhängigkeiten und Ausfallszenarien (Z 4). Die Leitfäden zu § 15 Abs. 2 Z 1 bis Z 6 RKEG konkretisieren dementsprechend nicht nur die Anforderungen in den einzelnen Maßnahmenbereichen, sondern setzen jeweils eine auf den konkreten Maßnahmenbereich bezogene Risikobetrachtung voraus, die über die allgemeine Risikoanalyse nach § 14 RKEG hinausgeht.

Zusammenspiel mit der NIS-2-Richtlinie

„Angelegenheiten, die in den Anwendungsbereich der Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (...) fallen, (NIS-2-Richtlinie), bleiben von diesem Bundesgesetz unberührt" (§ 2 Abs. 2 RKEG). Cybersicherheit und die unmittelbar damit verbundenen physischen Maßnahmen sind damit aus dem Anwendungsbereich des RKEG ausgenommen. Angesichts der engen Verbindung zwischen grundlegender physischer Sicherheit und Cybersicherheit kritischer Einrichtungen ist jedoch eine koordinierte Umsetzung beider Regelwerke sicherzustellen. Die RKE Richtlinie hält dazu fest, dass möglichst für einen kohärenten Ansatz zwischen beiden Richtlinien gesorgt werden soll.

Für die Praxis der Resilienzmaßnahmen bedeutet das: Bestehende Maßnahmen aus dem Bereich des Cybersicherheits-Risikomanagements gemäß NIS-2 sollen, soweit möglich, integriert und nicht parallel aufgebaut werden. Die Leitfäden nehmen an mehreren Stellen auf die Kohärenz mit NIS-2 Bezug; die konkrete Abgrenzung und Verzahnung wird in den jeweiligen Einzelleitfäden themenspezifisch behandelt.

Verhältnis zu sektoraler Regulierung

Soweit kritische Einrichtungen aufgrund sektorspezifischer Rechtsvorschriften der Union bereits Maßnahmen zur Verbesserung ihrer Resilienz treffen müssen und diese Anforderungen den Verpflichtungen aus dem RKEG als zumindest gleichwertig

anerkannt sind, finden die entsprechenden Bestimmungen des RKEG keine Anwendung. Dies dient der Vermeidung von Doppelgleisigkeiten.

Inhaltliche Grundlagen
Gemäß Art. 13 Abs. 5 RKE-RL hat die Europäische Kommission nicht-bindende Leitlinien zu erlassen, in denen die technischen, sicherheitsbezogenen und organisatorischen Resilienzmaßnahmen näher ausgeführt werden. Die Kommission hat auf dieser Grundlage nach Konsultation der Gruppe für die Resilienz kritischer Einrichtungen (Critical Entities Resilience Group – CERG) einen Entwurf für die „Guidelines on the application of Article 13(5) of the Directive (EU) 2022/2557 on the resilience of critical entities" (Stand März 2026) erarbeitet, der gemeinsam mit dem RKEG und den einschlägigen internationalen, europäischen und nationalen Normen und Richtlinien die inhaltliche Grundlage der vorliegenden Leitfäden bildet.

2 Anwendung der Leitfäden

Bestehende Regelungslage als Fundament
Grundlegend ist festzuhalten, dass Österreich bereits über eine dichte nationale und ausdifferenzierte sektorale Regulierung verfügt. In vielen der vom RKEG erfassten Sektoren bestehen umfangreiche gesetzliche, verordnungsrechtliche und behördliche Anforderungen, auf denen die Resilienzmaßnahmen aufbauen können. Der Regelungsgrad in den Sektoren ist dabei nicht einheitlich. Gut ausgebaut ist die Regelungslage beispielsweise in den Bereichen Anlagensicherheit und Betriebssicherheit (etwa durch die Gewerbeordnung, die Seveso-III-Umsetzung, das ArbeitnehmerInnenschutzgesetz, das Elektrotechnikgesetz oder die einschlägigen Betriebsanlagengenehmigungen) sowie im Brandschutz (durch Bauordnungen, TRVB-Richtlinien). In diesen Bereichen können kritische Einrichtungen in erheblichem Umfang auf bestehende Maßnahmen, Dokumentationen und Prüfmechanismen aufbauen.

Deutlich weniger oder gar nicht geregelt sind hingegen Bereiche wie der systematische physische Schutz gegen intentionale Bedrohungen, das Krisenmanagement oder die strukturierte Verknüpfung von Resilienzmaßnahmen zu einem dokumentierten Gesamtsystem.

Das RKEG ersetzt dabei die bestehenden Regelungen nicht und erfindet sie auch nicht neu. Es schafft einen sektorübergreifenden Resilienzrahmen, in den die bestehenden Anforderungen integriert werden, und ergänzt diesen dort, wo im Hinblick auf die Resilienz des wesentlichen Dienstes Lücken bestehen. Das Ziel ist eine nachvollziehbare Gesamtbetrachtung, die das vorhandene regulatorische Fundament mit den spezifischen Anforderungen des RKEG zusammenführt.

Wo bereits auf Grundlage bestehender Rechtsvorschriften Maßnahmen getroffen wurden, die den Anforderungen des § 15 RKEG entsprechen, sind diese Maßnahmen nicht zu duplizieren, sondern in den Resilienzrahmen einzubeziehen und als solche darzulegen. § 15 Abs. 3 RKEG stellt ausdrücklich klar, dass der Anforderung des

§ 15 Abs. 1 erster Satz RKEG insoweit entsprochen wird, als die kritische Einrichtung aufgrund anderer rechtlicher Verpflichtungen bereits gleichwertige Resilienzmaßnahmen ergriffen hat. Die Herausforderung liegt daher nicht darin, ein vollständig neues Maßnahmensystem aufzubauen, sondern darin, die vorhandenen Maßnahmen systematisch zu erfassen, auf den wesentlichen Dienst zu beziehen, auf ihre Vollständigkeit zu prüfen und dort gezielt zu ergänzen, wo der Resilienzrahmen des RKEG über die bisherige Regulierung hinausgeht.

Drei Säulen des Anforderungsrahmens

Die Anforderungen an die Resilienzmaßnahmen kritischer Einrichtungen ergeben sich aus dem Zusammenspiel dreier Säulen: dem RKEG als gesetzlicher Grundlage, den EU-Guidelines als inhaltlicher Konkretisierung sowie den einschlägigen europäischen und nationalen Normen und Richtlinien als technischem Umsetzungsrahmen. Die vorliegenden Leitfäden bringen diese drei Säulen zusammen und übersetzen sie für die kritischen Einrichtungen in einen anwendbaren Anforderungsrahmen.

Geeignetheit und Verhältnismäßigkeit

Das RKEG verlangt, dass kritische Einrichtungen „geeignete und verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen" treffen (§ 15 Abs. 1 RKEG). Diese beiden Begriffe definieren den zentralen Bewertungsmaßstab für sämtliche Resilienzmaßnahmen – sowohl für deren Planung durch die kritische Einrichtung als auch für deren Überprüfung durch die Behörde.

Geeignet (appropriate) bedeutet, dass die Maßnahmen risiko- oder wirkungsbasiert und so gestaltet sein sollen, dass sie eine umfassende Resilienz der kritischen Einrichtung bei der Erbringung der wesentlichen Dienste erreichen können. Die Geeignetheit einer Maßnahme kann sich, je nach deren spezifischen Gegebenheiten, zwischen verschiedenen kritischen Einrichtungen unterscheiden. Maßgeblich ist nicht eine abstrakte Tauglichkeit, sondern die tatsächliche Eignung im konkreten Risiko- und Betriebskontext der jeweiligen kritischen Einrichtung.

Verhältnismäßig (proportionate) bedeutet, dass die Maßnahmen notwendig und hinreichend, aber im Verhältnis zum Risiko und zur Schwere eines möglichen Sicherheitsvorfalles nicht übermäßig sein sollen. Die Verhältnismäßigkeit bemisst sich dabei nicht nur an der Schwere des Risikos, sondern auch an sondern auch an den konkreten Rahmenbedingungen der kritischen Einrichtung. Zu berücksichtigen sind insbesondere die Art des erbrachten wesentlichen Dienstes, die Lieferketten und Abhängigkeiten, die Wirtschaftlichkeit der Maßnahmen, die Größe der kritischen Einrichtung sowie die geografische Erstreckung des erbrachten Dienstes.

Die Beurteilung der Geeignetheit und Verhältnismäßigkeit erfolgt im Licht der Ergebnisse der nationalen Risikoanalyse gemäß § 10 RKEG sowie der einrichtungsinternen Risikoanalyse gemäß § 14 RKEG. Beide Risikoanalysen bilden den Referenzrahmen, an dem die Maßnahmengestaltung ausgerichtet und die Angemessenheit der gewählten Lösungen gemessen wird.

Konformitätsvermutung und Abweichung

Die in den Leitfäden formulierten Vorgaben folgen dem Verständnis, dass bei ihrer Einhaltung grundsätzlich von einer Konformität mit den Anforderungen des § 15 RKEG auszugehen ist. Die Anforderungen sollen daher grundsätzlich umgesetzt werden. Abweichungen von den Vorgaben der Leitfäden oder von den referenzierten Normen und Richtlinien sind zulässig, jedoch darzulegen: Die kritische Einrichtung hat nachvollziehbar zu begründen und zu dokumentieren, dass die gewählte alternative Lösung eine geeignete und verhältnismäßige Maßnahme im Sinne des § 15 Abs. 1 RKEG darstellt und eine gleichwertige Resilienzwirkung erreicht. Werden aufgrund betrieblicher, technischer, organisatorischer oder wirtschaftlicher Rahmenbedingungen andere Lösungen vorgesehen, sollen die Abweichungen konkret benannt, sachlich begründet und in ihrer alternativ erreichten Wirkung dargestellt werden. Je weiter eine Lösung von den Vorgaben des Leitfadens oder der einschlägigen Normen und Richtlinien entfernt ist, desto höher sind die Anforderungen an die Nachvollziehbarkeit und Belastbarkeit dieser Darlegung.

Für die behördliche Überprüfung ist wesentlich, dass nachvollziehbar dargelegt wird, wie die kritische Einrichtung die jeweiligen Anforderungen systemisch umgesetzt hat und an welchen Stellen mit welcher Begründung von den Vorgaben abgewichen wird. Nur auf dieser Grundlage sind sowohl die behördliche Überprüfung als auch die interne Steuerung und Weiterentwicklung der Resilienzmaßnahmen möglich.

Verhältnis zu Normen und Richtlinien

In Hinblick auf technische Ausgestaltung und Umsetzung verweisen die Leitfäden in weiten Teilen auf einschlägige europäische und nationale Normen. In diesen Fällen gelten die Normen und Richtlinien als anwendbare Regeln der Technik und sollen entsprechend herangezogen werden.

Dort, wo ein Leitfaden in Bezug auf die Normen und Richtlinien präzisierende, ergänzende oder abweichende Festlegungen trifft, gehen die Vorgaben des Leitfadens vor. Dies ist vor dem Hintergrund zu sehen, dass kritische Einrichtungen spezifische Anforderungen aufweisen, die in den bestehenden Normen und Richtlinien nicht vollständig abgedeckt sind – insbesondere hinsichtlich des Schutzniveaus, der sektorübergreifenden Abhängigkeiten und der besonderen Bedrohungslagen, denen kritische Einrichtungen ausgesetzt sein können. Die Leitfäden schließen diese Lücke, indem sie die normativen Vorgaben dort ergänzen oder anpassen, wo dies im Hinblick auf Resilienz kritischer Einrichtungen erforderlich ist. Solche Abweichungen und Präzisierungen sind in den Leitfäden gekennzeichnet und zur besseren Nachvollziehbarkeit im jeweiligen Anhang tabellarisch zusammengefasst.

Die in den Leitfäden enthaltenen Normenverweise beziehen sich auf den Stand 1. Juni 2026.

Die Orientierung an einschlägigen Normen und Richtlinien bzw. an definierten Anpassungen konkretisiert den Maßstab der Geeignetheit und Verhältnismäßigkeit: Wer eine Maßnahme entsprechend den Vorgaben der Leitfäden umsetzt, kann davon

ausgehen, dass diese den Anforderungen an eine geeignete und verhältnismäßige Resilienzmaßnahme entspricht.

Stufenlogik der behördlichen Prüfung

Die Pflicht zur Umsetzung geeigneter und verhältnismäßiger Resilienzmaßnahmen besteht ab dem in § 15 Abs. 1 RKEG festgelegten Zeitpunkt. Um dieser Pflicht erfolgreich nachzukommen, bedarf es sowohl belastbarer Konzepte als auch deren tatsächlicher Umsetzung. Da die Umsetzung ein tragfähiges Konzept voraussetzt, kommt der Entwicklung der konzeptionellen Grundlagen entscheidende Bedeutung zu.

Die jeweiligen Konzepte sind nicht bloß eine Vorstufe der Umsetzung, sondern das Fundament, auf dem alle weiteren Maßnahmen und Investitionen aufbauen. Sie machen den systemischen Zusammenhang der Resilienzmaßnahmen sichtbar und damit überhaupt erst beurteilbar. Ob eine Maßnahme geeignet und verhältnismäßig ist, lässt sich nicht anhand der Maßnahme allein beurteilen; sie entfaltet ihre Wirkung erst im Zusammenspiel mit den übrigen Elementen des Resilienzsystems. Erst die Konzepte zeigen, wie die einzelnen Maßnahmen zusammenwirken, welche Schutzziele sie gemeinsam erreichen und wo Lücken oder Redundanzen bestehen. Ohne belastbare, normativ fundierte Konzepte fehlt der Rahmen, in dem einzelne Maßnahmen sinnvoll verortet, priorisiert und in ihrer Angemessenheit bewertet werden können. Die konzeptionelle Grundlage bestimmt somit, ob Investitionen gezielt und zukunftsfähig erfolgen oder unkoordiniert und mit dem Risiko eines späteren Nachrüstungsbedarfs.

Aus diesem Grund sollen sämtliche Investitionen in Resilienzmaßnahmen von Beginn an konsequent unter dem Blickwinkel der einschlägigen normativen Grundlagen betrachtet werden. Das betrifft insbesondere technische Investitionen (etwa in Einbruchmeldeanlagen, Zutrittskontrollsysteme, Videoüberwachung oder bauliche Schutzmaßnahmen). Wer bei solchen Investitionen die normative Orientierung von Beginn an mitdenkt, schafft belastbare Lösungen.

3 Aufbau und Zusammenhang der Leitfäden

Die Leitfäden zu § 15 Abs. 2 RKEG bestehen aus sieben Teilen: einem allgemeinen Leitfaden (Z 0), der die übergreifenden Grundlagen für alle Einzelleitfäden enthält, sowie sechs Einzelleitfäden, die unmittelbar auf § 15 Abs. 2 Z 1 bis Z 6 RKEG abzielen.
Der Gesamtaufbau ist wie folgt:

Allgemeine Grundlagen und Anwendung des Leitfadens (Z 0): rechtlicher Rahmen, Maßstab der Geeignetheit und Verhältnismäßigkeit, Konformitätsvermutung, Normenverhältnis sowie allgemeine Grundsätze für Resilienzmaßnahmen
Verhinderung von Sicherheitsvorfällen (Z 1): Verhinderung von Sicherheitsvorfällen durch technische, anlagentechnische, betriebliche, organisatorische und personelle Maßnahmen, einschließlich Katastrophenvorsorge und Anpassung an den Klimawandel
Physischer Schutz (Z 2): Gewährleistung eines angemessenen physischen Schutzes der kritischen Infrastruktur und der Räumlichkeiten durch bauliche, mechanische, elektronische, organisatorische und personelle Schutzmaßnahmen
Abwehr und Bewältigung von Sicherheitsvorfällen (Z 3): Abwehr von Sicherheitsvorfällen, deren Bewältigung sowie möglichst weitgehende Begrenzung der Auswirkungen durch Reaktions- und Führungsfähigkeit, Kommunikation, Wirkungsminimierung und Ressourcensteuerung
Fortsetzung und rasche Wiederaufnahme nach Sicherheitsvorfällen (Z 4): Sicherstellung der Fortsetzung oder raschen Wiederaufnahme des wesentlichen Dienstes durch Business Continuity Management, Wiederanlaufplanung, Ressourcen- und Redundanzplanung sowie Berücksichtigung alternativer Lieferketten
Personelle Sicherheitsvorkehrungen (Z 5): angemessene personelle Sicherheitsvorkehrungen durch Identifikation kritischer Funktionen, Steuerung von Zugangsberechtigungen, Zuverlässigkeitsüberprüfungen und Festlegung von Ausbildungs- und Qualifikationsanforderungen
Sensibilisierung und Schulung (Z 6): Sensibilisierung des Personals in kritischen Funktionen durch Schulungsmaßnahmen, Informationsmaterialien und Übungen, die den gesamten Resilienzkreislauf abdecken

Diese sieben Leitfäden bilden kein isoliertes Nebeneinander von Einzelmaßnahmen, sondern ein zusammenhängendes System, das den gesamten Resilienzkreislauf einer kritischen Einrichtung abdeckt. Resilienz entsteht erst im Zusammenspiel aller Elemente. Einzelne Maßnahmen können isoliert weder hinsichtlich ihrer Wirkung noch hinsichtlich ihrer Verhältnismäßigkeit abschließend bewertet werden. Resilienzmaßnahmen sollen daher als Teile eines integrierten Systems und nicht als isolierte Einzelmaßnahmen betrachtet werden.

4 Allgemeine Grundsätze für Resilienzmaßnahmen

Die folgenden Grundsätze gelten übergreifend für alle Resilienzmaßnahmen gemäß § 15 Abs. 2 Z 1 bis Z 6 RKEG.

Resilienz als Führungsaufgabe
Resilienz ist keine operative Einzelaufgabe, sondern eine Führungsverantwortung, die auf allen Ebenen einer Einrichtung verankert sein muss. Kritische Einrichtungen sollen Resilienzziele festlegen, Strategie, Policy und Planung für Resilienz beschließen, diese den relevanten Interessenträgern gemäß dem Need-to-know-Prinzip kommunizieren und regelmäßig überprüfen. Dabei sollen bestehende Schwachstellen und Möglichkeiten berücksichtigt werden, wie Vorfälle besser verhindert, abgewehrt, bewältigt und ihre Auswirkungen begrenzt werden können.

Angemessene Resilienzkompetenz soll auf Ebene der obersten Leitung sowie in Resilienz- oder Risikomanagementfunktionen gebündelt werden, um eine ausreichende strategische und operative Resilienzplanung sicherzustellen. Kritische Einrichtungen sollen prüfen, ob die Bestellung eines Resilienzbeauftragten sinnvoll ist, der die koordinierenden Rollen und Zuständigkeiten für die Umsetzung der Resilienzziele klar bündelt. Dafür sollen klare Entscheidungshierarchien eingerichtet werden.

Resilienzplan und Dokumentation
Kritische Einrichtungen haben die von ihnen getroffenen Maßnahmen in einem Resilienzplan nachvollziehbar darzulegen (§ 15 Abs. 1 RKEG). Der Resilienzplan stellt das zentrale Steuerungsinstrument dar, auf das die Gesamtkonzepte der einzelnen Leitfäden aufbauen. Der Detaillierungsgrad soll hinreichend sein, um die Ziele der Wirksamkeit und Nachvollziehbarkeit zu erreichen. Etwaige Ausnahmen davon sind in § 18 RKEG angeführt.

Zusammenarbeit mit Behörden und privaten Akteuren
Kritische Einrichtungen sollen die Zusammenarbeit mit einschlägigen Behörden (wie Strafverfolgung) sowie Einsatzorganisationen (wie Feuerwehr und Rettungsdiensten) etablieren und formalisieren. Rollen und Verfahren für den Informationsaustausch, die Meldung und Koordination von Sicherheitsvorfällen sowie die gegenseitigen Erwartungen sollen klar geregelt sein. Darüber hinaus kann auch die Zusammenarbeit mit relevanten privatwirtschaftlichen Akteuren im eigenen Sektor, in anderen Sektoren und in anderen Mitgliedstaaten in Betracht gezogen werden.

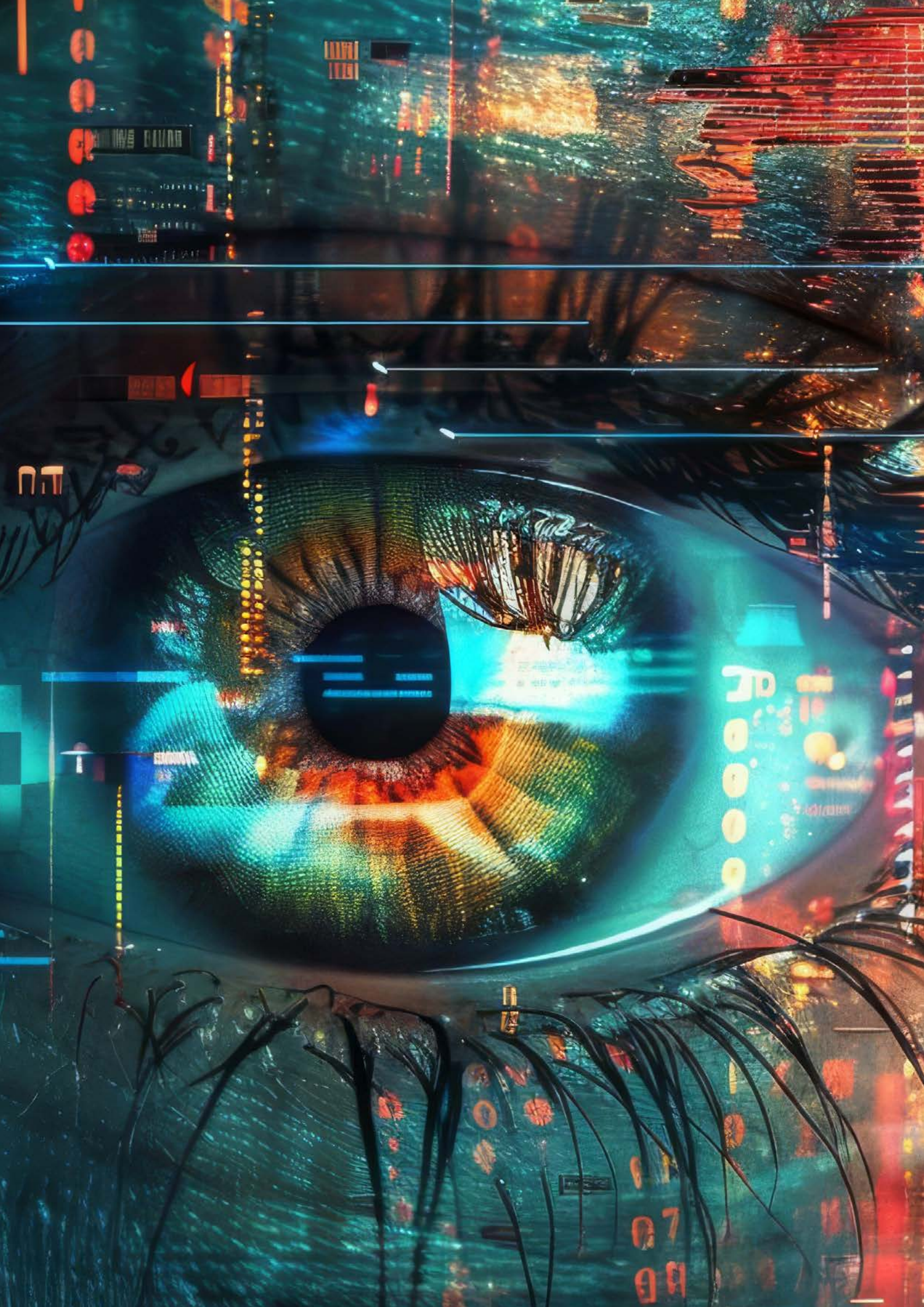
Kohärenz im Maßnahmenbereich
Die Resilienzmaßnahmen gemäß § 15 RKEG sind unbeschadet und in Kohärenz mit den Maßnahmen zu treffen, die sich aus einschlägigen sektoralen Rechtsvorschriften ergeben. Bestehende Maßnahmen sollen – soweit sie den Anforderungen des RKEG entsprechen – integriert und nicht parallel aufgebaut werden. Dies gilt insbesondere für Maßnahmen im Bereich des Cybersicherheits-Risikomanagements gemäß NIS-2. Soweit für IKT-Sicherheit einschlägige Vorgaben bestehen, insbesondere aus der Durch-

führungsverordnung (EU) 2024/2690 und der begleitenden ENISA-Umsetzungsanleitung, sollen diese ergänzend berücksichtigt werden.

Einsatz künstlicher Intelligenz (KI)
Soweit kritische Einrichtungen KI-Systeme im Rahmen ihrer Resilienzmaßnahmen einsetzen, ist zu beachten, dass diese den Sicherheits- und Resilienzanforderungen der KI-Verordnung (EU) 2024/1689 entsprechen müssen. Die KI-Verordnung stuft KI-Systeme, die als Sicherheitskomponenten in der Verwaltung und dem Betrieb kritischer digitaler Infrastruktur, im Straßenverkehr oder in der Wasser-, Gas-, Wärme- oder Stromversorgung eingesetzt werden sollen, als Hochrisiko-KI-Systeme ein.

Ganzheitlicher Ansatz und einrichtungsinterne Risikoanalyse
Kritische Einrichtungen sollen einen ganzheitlichen Ansatz verfolgen und den Übergang vom bloßen Schutz der kritischen Infrastruktur zur Sicherstellung der Kontinuität des erbrachten wesentlichen Dienstes vollziehen. Die Ergebnisse der einrichtungsinternen Risikoanalyse gemäß § 14 RKEG sollen unmittelbar mit den Resilienzmaßnahmen verknüpft werden. Die einrichtungsinterne Risikoanalyse soll nicht nur die unmittelbaren Abhängigkeiten der Einrichtung erfassen, sondern auch beurteilen und berücksichtigen, inwieweit andere Sektoren vom wesentlichen Dienst der kritischen Einrichtung abhängen und inwieweit die kritische Einrichtung von wesentlichen Diensten abhängt, die von Einrichtungen in anderen Sektoren erbracht werden – gegebenenfalls auch in benachbarten Mitgliedstaaten und Drittstaaten.
Im Rahmen der Planung und Umsetzung von Resilienzmaßnahmen sollen kritische Einrichtungen alle relevanten Anlagen, Einrichtungen und Ausrüstungen identifizieren und dabei grenzüberschreitende Aspekte sowie Interdependenzen berücksichtigen (einschließlich physischer, umweltbezogener, cyberbezogener und lieferkettenbezogener Abhängigkeiten). Die Vernetzung der vom RKEG erfassten Sektoren bringt mit sich, dass eine Störung in einem Bereich kaskadierende Auswirkungen auf andere Bereiche haben und die Erbringung wesentlicher Dienste beeinträchtigen kann.

Sektorbezogenheit
Die Leitfäden sind sektorübergreifend angelegt und enthalten horizontale Anforderungen, die grundsätzlich für alle vom RKEG erfassten Sektoren und Teilsektoren gelten. Die darin angeführten Maßnahmen und Beispiele erheben keinen Anspruch auf Vollständigkeit und können nicht gleichermaßen auf alle Sektoren und alle Arten kritischer Infrastruktur angewendet werden. Die konkrete Ausgestaltung der Maßnahmen muss daher stets sektorbezogen erfolgen und die spezifischen Gegebenheiten des jeweiligen wesentlichen Dienstes, der betrieblichen Rahmenbedingungen und der sektoralen Regulierung berücksichtigen. Eine Maßnahme, die in einem Sektor geeignet und wirksam ist, kann in einem anderen Sektor unverhältnismäßig oder ungeeignet sein.



Z 1: Verhinderung von Sicherheitsvorfällen

In Kooperation mit DCNAustria
Disaster Competence Network Austria

1 Allgemeine Grundlagen

Kritische Einrichtungen haben geeignete und verhältnismäßige Resilienzmaßnahmen zu treffen, um das Auftreten von Sicherheitsvorfällen zu verhindern. Dies umfasst insbesondere Maßnahmen zur Betriebssicherheit und Katastrophenvorsorge sowie zum Umgang mit dem Klimawandel.

Prävention ist dabei nicht als Summe einzelner Schutzvorkehrungen zu verstehen, sondern als integrierter Ansatz zur Vermeidung, Begrenzung und frühzeitigen Beherrschung von Störungen. Diese Maßnahmen sollen als Teil eines integrierten Systems betrachtet werden.

Die Wirksamkeit jeder einzelnen Maßnahme hängt von ihrer Wechselwirkung mit anderen Maßnahmen ab, etwa solchen zum physischen Schutz der Räumlichkeiten, zur Abwehr und Bewältigung von Sicherheitsvorfällen, zur Begrenzung ihrer Auswirkungen sowie zur Gewährleistung einer angemessenen personellen Sicherheit. Ein integrierter Präventionsansatz bedeutet daher, dass unterschiedliche Schutzebenen und Barrieren in funktionalem Zusammenhang geplant werden. Technische Schutzmaßnahmen, sichere Betriebsführung, Instandhaltung, Überwachung, personelle Absicherung und vorsorgliche Eingriffsmechanismen sind nicht getrennt zu betrachten, sondern als aufeinander bezogene Bestandteile eines gemeinsamen Präventionssystems.

Dieser Systemgedanke ist insbesondere dort von Bedeutung, wo einzelne Schwachstellen oder Ausfälle nicht unmittelbar zu einer Störung des wesentlichen Dienstes führen, jedoch im Zusammenwirken mit weiteren Defiziten oder Belastungen erhebliche Auswirkungen entfalten können. Eine kritische Einrichtung kann etwa über robuste technische Schutzmaßnahmen verfügen, die dennoch unter Belastungslagen nicht voll wirksam werden können, wenn klare Betriebsverfahren, verlässliche Zuständigkeiten, ausreichende Instandhaltung oder frühzeitige Warn- und Eingriffsmechanismen fehlen. Umgekehrt können organisatorische oder personelle Maßnahmen technische Schutzdefizite nicht vollständig kompensieren. Ein wirksames Präventionssystem setzt daher mehrere, aufeinander abgestimmte Schutz- und Sicherheitsbarrieren voraus.

In diesem Zusammenhang ist auch zu berücksichtigen, dass Maßnahmen zur Sicherung der physischen Systemintegrität nicht ausschließlich als Katastrophenvorsorge einzuordnen sind. Die Erhaltung der Betriebssicherheit sowie von Trag-, Schutz-, Dichtheits- und Funktionseigenschaften von Gebäuden, Anlagen und technischen Einrichtungen ist zugleich eine grundlegende Voraussetzung dafür, dass Ausfälle und Störungen gar nicht erst eintreten.

Der vorliegende Leitfaden behandelt die Verhinderung von Sicherheitsvorfällen entlang folgender Schwerpunkte: Zunächst werden allgemeine Maßnahmen zur Prävention von Ausfällen und Störungen dargestellt, die technische, anlagentechnische und betriebliche Vorkehrungen umfassen. Daran schließen Maßnahmen zur Katastrophenvorsorge und strukturellen Härtung an, gefolgt von der Klimawandelanpassung als eigenständigem Handlungsfeld mit langfristiger Perspektive.

Ergänzend werden die Erfassung von Ereignissen und systematisches Lernen aus Vorfällen sowie die Verhinderung menschlicher Fehler behandelt.

Die in diesem Leitfaden beschriebenen Maßnahmen gelten unbeschadet der Verpflichtungen zum Cybersicherheits-Risikomanagement. Für die IKT-Sicherheit sind die einschlägigen Vorgaben und Maßnahmen heranzuziehen. Bestehende Maßnahmen aus diesem Bereich sollten, soweit möglich, integriert und nicht parallel aufgebaut werden.

2 Prävention von Ausfällen und Störungen

In den kritischen Einrichtungen Österreichs ist durch bestehende gesetzliche Vorgaben bereits ein hohes Niveau an technischer Sicherheit vorhanden. Die folgenden Kapitel dieses Leitfadens Z 1 sind unter diesem Gesichtspunkt zu verstehen. Die beschriebenen Maßnahmen orientieren sich ausschließlich am wesentlichen Dienst der kritischen Einrichtungen.

Ziel präventiver Maßnahmen ist es, Sicherheitsvorfälle möglichst zu verhindern oder ihre Eintrittswahrscheinlichkeit wesentlich zu verringern. Dies umfasst insbesondere die Vermeidung unsicherer Betriebszustände, den Erhalt sicherheitsrelevanter Funktionen, die Begrenzung technischer und organisatorischer Schwachstellen sowie die Verhinderung von Ereignissen, die zu Brand-, Explosions-, Freisetzungs- oder sonstigen schweren Störungslagen führen können, welche die Erbringung des wesentlichen Dienstes beeinträchtigen.

Prävention setzt zeitlich und funktional vor Reaktion, Bewältigung und Wiederherstellung an. Die Auswahl und Ausgestaltung von Präventionsmaßnahmen hat sich nicht allein an isolierten Gefährdungen oder Einzelfunktionen zu orientieren, sondern an der Frage, wie die für den wesentlichen Dienst maßgeblichen Systeme, Prozesse und Betriebsbedingungen in ihrer Gesamtheit stabil und beherrschbar gehalten werden können.

2.1 Technische Prävention und Anlagensicherheit

Technische Präventionsmaßnahmen sind alle baulichen, konstruktiven, anlagen- und ausrüstungstechnischen Vorkehrungen, die darauf ausgerichtet sind, Sicherheitsvorfälle bereits im Vorfeld zu vermeiden oder ihre Eintrittswahrscheinlichkeit zu reduzieren. Sie bilden die primäre materielle Schutzebene gegen störungsauslösende Einwirkungen.

Technische Präventionsmaßnahmen betreffen insbesondere die baulich-technische Auslegung, Anordnung, Ausstattung und physische Absicherung von Gebäuden, Anlagen, Anlagenteilen und Infrastrukturelementen. Dazu gehören vor allem robuste Auslegung kritischer Komponenten, räumliche Trennung besonders empfindlicher oder störanfälliger Bereiche, bauliche Abschottungen, Abdichtungen, Rückhalteeinrichtungen, Schutz gegen Überflutung, Hitze, mechanische Einwirkungen oder Medienaustritt sowie Ersatzversorgungen, Notstromsysteme und redundante Auslegung

technischer Funktionen. Vorhandene Vorkehrungen aus dem Bereich Operational Safety können als Grundlage für Maßnahmen zur Absicherung der Erbringung des wesentlichen Dienstes dienen, sollten aber in Hinblick auf diese Zielsetzung überprüft werden.

Maßgeblich ist, dass solche Maßnahmen früh in der Kette möglicher Störungsursachen ansetzen. Ihre Eignung ist danach zu beurteilen, ob sie relevante Belastungen und Ausfallmechanismen bereits auf der Ebene der technischen Auslegung und Ausstattung wirksam begrenzen.

Über die allgemeine technische Prävention hinaus umfasst die Anlagen- und Prozesssicherheit jene Vorkehrungen, die darauf gerichtet sind, Anlagen und betriebliche Prozesse innerhalb sicherer Betriebsgrenzen zu halten und das Entstehen unzulässiger, gefahrenträchtiger oder nicht mehr beherrschbarer Zustände zu verhindern. Im Mittelpunkt steht die sichere Beherrschung von Stoff-, Energie- und Prozesszuständen, deren Abweichung den wesentlichen Dienst beeinträchtigen oder zu schweren Störungslagen führen kann.

Ein zentraler Gegenstand ist die Vermeidung von Ereignissen, die aus dem Verlust der Beherrschung von Stoffen, Energien oder technischen Zuständen entstehen können. Im Rahmen der Prävention sollen kritische Einrichtungen Maßnahmen treffen, um Kollisionen, Explosionen, Freisetzungen gefährlicher Stoffe und von Strahlung zu verhindern. Dazu zählen insbesondere Brände, Leckagen, Überfüllungen, unzulässige Reaktionen, thermische Überlastungen, Drucküberschreitungen und Fehlsteuerungen. Präventive Maßnahmen müssen darauf gerichtet sein, das Entstehen solcher Zustände möglichst nicht zuzulassen und erkennbare Abweichungen vor einer Eskalation zu beherrschen.

Dies setzt voraus, dass für sicherheitsrelevante Abweichungen wirksame Sicherheitsfunktionen vorhanden sind: Mess-, Steuer- und Regeleinrichtungen, Verriegelungen, Interlocks, Abschaltungen, Füllstandsbegrenzungen, Leckageerkennung, Druckentlastung, Temperatur- und Drucküberwachung, Not-Aus-Funktionen sowie sonstige Schutzfunktionen, die ein Überschreiten sicherer Betriebsgrenzen verhindern oder die Anlage rechtzeitig in einen sicheren Zustand überführen. Maßgeblich ist, dass diese Funktionen nicht nur vorhanden, sondern für die relevanten Abweichungsszenarien geeignet, zuverlässig und in ihrer Schutzwirkung nachvollziehbar sind.

Die Beurteilung der Anlagen- und Prozesssicherheit hat stets systemisch zu erfolgen. Zu berücksichtigen ist das Zusammenwirken von Hauptfunktionen, Hilfs- und Nebensystemen, Energie- und Medienversorgung, Steuerungsfunktionen und Bedienhandlungen. Schwächen in Hilfssystemen oder Versorgungsfunktionen können ebenso zum Verlust sicherer Betriebszustände führen wie Defizite in Hauptanlagen.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
OVE EN 61511 -x (Reihe)	Functional safety – Safety instrumented systems for the process industry sector
ÖNORM EN 1127-1	Explosionsfähige Atmosphären – Explosionsschutz - Teil 1: Grundlagen und Methodik
ÖNORM EN 764-7	Druckgeräte – Teil 7: Sicherheitseinrichtungen für unbefeuerte Druckgeräte

Stand: 01. Juni 2026

Tipps

Bestehende technische Schutzkonzepte sollen herangezogen werden, etwa Brandschutz, Explosionsschutz, Prozesssicherheit, Rückhaltung, Leckageerkennung, Not-Aus-Funktionen, Interlocks, Verriegelungen oder redundante Versorgungssysteme.
Für das RKEG soll geprüft werden, ob diese Maßnahmen auch unter Störungsbedingungen verfügbar bleiben und den wesentlichen Dienst ausreichend schützen. Hilfs- und Nebensysteme wie Energieversorgung, Kühlung, Steuerung, Kommunikation, Entwässerung oder Druckluft sollen ausdrücklich mitbewertet werden.

2.2 Sichere Betriebsführung und Instandhaltung

Sichere Betriebsführung und Standardverfahren dienen dazu, kritische Infrastrukturen unter definierten, nachvollziehbaren und beherrschbaren Bedingungen zu führen. Ziel ist es, sicherheits- und resilienzrelevante Tätigkeiten so zu organisieren, dass unzulässige Zustände nicht durch unsichere Bedienung, ungeordnete Eingriffe oder uneinheitliche Vorgehensweisen begünstigt werden.

Sichere Betriebsführung betrifft insbesondere das An- und Abfahren von Anlagen, Umschaltungen, Freigaben, Wiederinbetriebnahmen, Eingriffe in laufende Prozesse, Tätigkeiten bei eingeschränkten Betriebszuständen sowie den Übergang in notbetriebliche Betriebsformen. Maßgeblich ist, dass solche Vorgänge nicht improvisiert erfolgen, sondern auf vorbereiteten und abgestimmten Handlungslogiken beruhen.

Standardverfahren bilden hierfür die operative Grundlage. Dazu gehören insbesondere Betriebsanweisungen, Verfahrensanweisungen, Freigabeprozesse, Checklisten, Schalt- und Umschaltpläne, Melde- und Eskalationswege sowie definierte Reaktionsschritte für Abweichungen und Warnlagen. Von besonderer Bedeutung ist, dass Zuständigkeiten, Entscheidungsbefugnisse und Schnittstellen eindeutig geregelt sind.

Standardverfahren müssen nicht nur für den Normalbetrieb, sondern auch für Warnlagen, eingeschränkte Betriebszustände, kontrollierte Abschaltungen, Notbetrieb und Wiederanlauf vorhanden sein.

Wartung, Instandhaltung, Prüfung und Monitoring ergänzen die sichere Betriebsführung um die dauerhafte Erhaltung, Überprüfung und zustandsbezogene Bewertung präventiver Resilienzmaßnahmen. Ziel ist es, schleichende Verschlechterungen, Ausfalltendenzen, Integritätsverluste und Funktionsabweichungen frühzeitig zu erkennen, zu dokumentieren und rechtzeitig zu beheben.

Wartung und Instandhaltung umfassen alle Maßnahmen zur Erhaltung oder Wiederherstellung des bestimmungsgemäßen Zustands sicherheits- und resilienzrelevanter Systeme und Komponenten. Instandhaltung ist dabei nicht nur als Störungsbehebung, sondern als planmäßige Erhaltungsmaßnahme zur Sicherung technischer Verfügbarkeit und Integrität zu verstehen.

Prüfung umfasst die planmäßige und anlassbezogene Feststellung, ob sicherheits- und resilienzrelevante Systeme die an sie gestellten Anforderungen weiterhin erfüllen. Dazu gehören Inspektionen, Funktionsprüfungen, Dichtheitsprüfungen, Kalibrierungen und Wirksamkeitskontrollen. Prüfungen dienen damit nicht nur der technischen Kontrolle, sondern auch der Nachweisführung.

Wartung, Instandhaltung sowie Prüfung sind risikobasiert und funktionsbezogen auszugestalten. Vorrangig zu betrachten sind jene kritischen Infrastrukturen, deren Ausfall oder schleichende Verschlechterung erhebliche Auswirkungen auf kritische Funktionen oder den wesentlichen Dienst haben kann.

Die aus dem diesem Monitoring gewonnenen Daten und Beobachtungen bilden die Grundlage für die Früherkennung kritischer Entwicklungen und vorsorgliche Eingriffsmechanismen, die im Leitfaden Z 1, Kapitel 2.4 behandelt werden.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ISO 55001	Asset management – Management systems – Requirements
ÖNORM B 1301	Objektsicherheitsprüfungen für Nicht-Wohngebäude – Regelmäßige Prüfroutinen im Rahmen von Sichtkontrollen und Begutachtungen – Grundlagen und Checklisten
ÖVE/ÖNORM EN 50110-1	Betrieb von elektrischen Anlagen – Teil 1 Allgemeine Anforderungen
OVE EN 50160	Voltage characteristics of electricity supplied by public electricity networks
IEC 62682	Alarmmanagement in der Prozessindustrie

Stand: 01. Juni 2026

Tipps

Betriebsanweisungen, Checklisten, Schaltpläne, Freigabeprozesse, Prüfpläne und Instandhaltungsprogramme sollen auf ihre resilienzrelevante Wirkung geprüft werden.
Instandhaltung soll risikobasiert priorisiert werden. Vorrang haben Komponenten, deren Ausfall die Erbringung des wesentlichen Dienstes beeinträchtigen kann.
Prüf- und Wartungsintervalle sollen anhand von Betriebserfahrung, Alterung, Störungsdaten, Belastung und Kritikalität bewertet werden.

2.3 Vermeidung kritischer Einzelabhängigkeiten

Die Vermeidung von Single Points of Failure ist ein zentrales Prinzip präventiver Resilienzmaßnahmen. Gemeint sind einzelne Komponenten, Funktionen, Prozesse, Ressourcen, Standorte, Schnittstellen oder personelle Schlüsselstellen, deren Ausfall unmittelbar oder mittelbar zu einer erheblichen Beeinträchtigung des wesentlichen Dienstes führen kann. Solche Einzelabhängigkeiten stellen eine besondere Verwundbarkeit dar, weil die Stabilität des Gesamtsystems in unverhältnismäßiger Weise an die Verfügbarkeit eines einzigen Elements gebunden wird.

Single Points of Failure können technischer, organisatorischer, infrastruktureller, digitaler oder personeller Natur sein. Sie können in Hauptsystemen ebenso vorliegen wie in Hilfs-, Neben- oder Unterstützungsfunktionen, deren Bedeutung im Normalbetrieb häufig unterschätzt wird. Gerade Hilfsenergieversorgung, Kühlung, Entwässerung, Telekommunikation, Mess- und Übertragungseinrichtungen, lokale Bedienmöglichkeiten oder personelle Entscheidungs- und Eingriffsbefugnisse können im Ereignisfall zu kritischen Engstellen werden.

Maßgeblich ist nicht nur, ob ein einzelnes Element formell vorhanden ist, sondern ob sein Ausfall in realistischer Weise kompensiert, überbrückt oder beherrscht werden kann. Ebenso ist zu bewerten, ob vorhandene Redundanzen tatsächlich unabhängig, belastbar und unter Störungsbedingungen nutzbar sind. Formale Mehrfachauslegung genügt nicht, wenn redundante Systeme denselben Gefährdungen unterliegen, räumlich zu nahe beieinander angeordnet sind, von derselben Hilfsfunktion abhängen oder im Ereignisfall nicht rechtzeitig verfügbar gemacht werden können.

Die Vermeidung solcher Einzelabhängigkeiten bedeutet nicht zwingend, dass alle kritischen Elemente (Komponenten, Systeme, Prozesse oder Schnittstellen), deren Ausfall die Erbringung des wesentlichen Dienstes unmittelbar beeinträchtigt, redundant ausgestaltet werden müssen. Erforderlich sind vielmehr geeignete und verhältnismäßige Lösungen, mit denen die Ausfallwirkung eines einzelnen Elements begrenzt oder beherrschbar gemacht wird. Dies kann etwa durch technische Redundanz, räumliche Trennung, Diversifizierung von Versorgungswegen, alternative Betriebs- oder Steuerungspfade, Ersatzsysteme, Notbetriebsoptionen, Bevorratung kritischer Ersatzteile, alternative Lieferquellen, unabhängige Kommunikationswege, lokale Bedienmöglichkeiten oder manuelle Rückfallebenen erfolgen.

Die Vermeidung von Single Points of Failure ist als querschnittsbezogene Prüffrage des gesamten Präventionssystems zu verstehen. Einrichtungen haben ihre kritischen Funktionen, Prozesse, Infrastrukturelemente, Schnittstellen und personellen Schlüsselrollen systematisch dahingehend zu untersuchen, wo ausfallkritische Einzelabhängigkeiten bestehen und wie diese reduziert werden können. Der Fokus liegt dabei auf der Vermeidung von Ausfällen. Die Bewältigung eingetretener Ausfälle und die Sicherstellung alternativer Lieferketten sind Gegenstand der Kontinuität des wesentlichen Dienstes und werden im entsprechenden Kapitel behandelt.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖNORM EN ISO 22301	Sicherheit und Resilienz – Business Continuity – Management System – Anforderungen
ÖNORM ISO 31000	Risikomanagement – Leitlinien

Stand: 01. Juni 2026

Tipps

Auch Nebenfunktionen wie Kühlung, Entwässerung, Notstrom, Telekommunikation, Ersatzteile, lokale Bedienmöglichkeiten oder Schlüsselpersonal können kritisch sein. Vorhandene Redundanzen sollen auf tatsächliche Unabhängigkeit geprüft werden. Nicht jede Einzelabhängigkeit erfordert vollständige Redudanz. Auch alternative Betriebsweisen, manuelle Rückfallebenen, mobile Systeme oder vertraglich gesicherte Unterstützung können geeignet sein.

2.4 Früherkennung und vorsorgliche Eingriffsmechanismen

Ein wesentlicher Bestandteil präventiver Resilienzmaßnahmen ist die Fähigkeit, kritische Entwicklungen, Vorwarnlagen und sich anbahnende Störungen frühzeitig zu erkennen und noch vor Eintritt erheblicher Auswirkungen geeignete Maßnahmen auszulösen. Früherkennung und vorsorgliche Eingriffsmechanismen bilden die operative Brücke zwischen allgemeiner Prävention und aktiver Beherrschung beginnender Störungslagen.

Früherkennung umfasst alle technischen, organisatorischen und prozessualen Mittel, durch die relevante Veränderungen, Anzeichen oder Belastungsentwicklungen rechtzeitig sichtbar gemacht werden. Dazu gehören insbesondere Warn- und Meldesysteme, Zustandsüberwachung, Prozess- und Integritätsmonitoring, Trendanalysen, Schwellenwertüberwachung, Umwelt- und Wetterbeobachtung, Störmeldungen sowie die systematische Nutzung interner und externer Informationen zu Gefährdungen und Belastungen.

Die Wirksamkeit der Früherkennung hängt wesentlich davon ab, dass relevante Indikatoren bekannt, Schwellenwerte definiert und Zuständigkeiten für Bewertung und Maßnahmenauslösung eindeutig festgelegt sind. Sonst besteht die Gefahr, dass

relevante Hinweise verspätet, uneinheitlich oder gar nicht in wirksame Maßnahmen umgesetzt werden.

Vorsorgliche Eingriffsmechanismen sind die daran anknüpfenden, vorab festgelegten Maßnahmen, die bei erkannten Vorzeichen oder absehbaren Belastungen ausgelöst werden können. Dazu gehören insbesondere die Aktivierung technischer Schutzfunktionen, das Umschalten auf robustere oder sichere Betriebszustände, die vorsorgliche Reduktion von Lasten oder Durchsätzen, die kontrollierte Außerbetriebnahme besonders gefährdeter Teilfunktionen, personelle Verstärkungen sowie der frühzeitige Übergang in eingeschränkte Betriebsformen oder vorbereitete Notbetriebsformen.

Hochautomatisierte Systeme können Effizienz und Stabilität erhöhen, schaffen aber neue Verwundbarkeiten, wenn menschliche Eingriffe im Störungsfall nicht oder nicht rechtzeitig möglich sind. Bei operativer Technologie sollen manuelle Übersteuerungen und Vorkehrungen für menschliche Eingriffe vorgesehen werden, wobei die konkreten Bedingungen und Anforderungen für menschliche Intervention und manuelle Steuerung als Reaktion auf Gefährdungen festzulegen sind. Diese Integration von Human-in-the-Loop bedeutet, dass menschliche Entscheidung und Kontrolle in sicherheits- oder resilienzrelevanten Situationen gezielt eingebunden bleiben. Dazu ist festzulegen, unter welchen konkreten Bedingungen ein manueller Eingriff vorgesehen ist, welche Voraussetzungen dafür erfüllt sein müssen (Informationslage, Zugänglichkeit, Qualifikation), welche Personen zur Übersteuerung befugt sind und welche Entscheidungskriterien dabei gelten. Dabei ist insbesondere auf die Bedeutung von regelmäßigem Training hinzuweisen, denn manuelle Übersteuerungsmöglichkeiten sind nur dann wirksam, wenn das Personal sie regelmäßig übt. Ein manueller Eingriff, der nur auf dem Papier existiert und nie unter realistischen Bedingungen getestet wurde, wird im Ereignisfall mit hoher Wahrscheinlichkeit scheitern. Manuelle Rückfallebenen sollen daher in regelmäßige Übungsszenarien einbezogen werden, insbesondere unter Zeitdruck oder Bedingungen eingeschränkter Informationslage.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
OVE EN IEC 62682	Alarmmanagement in der Prozessindustrie
API RP 754	Process Safety Performance Indicators for the Refining and Petrochemical Industries
OVE EN 61511-x	Functional safety – Safety instrumented systems for the process industry sector (Reihe)

Stand: 01. Juni 2026

Tipps

Vorsorgliche Eingriffe sollen möglichst vor Eintritt der eigentlichen Störung ansetzen, etwa durch Lastreduktion, Umschaltung, zusätzliche Kontrollen oder kontrollierte Außerbetriebnahme.
Warnsignale sollen mit klaren Schwellenwerten, Zuständigkeiten und Maßnahmen verknüpft werden.
Manuelle Rückfallebenen sollen geübt werden, damit Personal, Zugang, Information, Befugnis und Training im Ereignisfall tatsächlich vorhanden sind.

3 Katastrophenvorsorge und strukturelle Härtung

Kritische Einrichtungen haben nicht nur betriebsinterne Ausfallursachen zu beherrschen, sondern auch äußere Einwirkungen zu berücksichtigen, die die Integrität von Gebäuden, Anlagen und betriebsnotwendigen Infrastrukturelementen beeinträchtigen können. Hierzu zählen insbesondere Naturgefahren, klimabedingte Belastungen und standortbezogene Expositionen mit potenziell erheblichen Auswirkungen auf den wesentlichen Dienst.

Kritische Einrichtungen sollen Maßnahmen zur Katastrophenrisikoreduzierung und zur Klimawandelanpassung treffen. Dieser Leitfadenabschnitt behandelt die kurzfristig und strukturell wirksamen Maßnahmen der Katastrophenvorsorge. Die langfristige Klimawandelanpassung wird in einem eigenen Kapitel dargestellt.

3.1 Standortwahl und Expositionsminderung

Die Vermeidung hochgefährdeter Standorte für kritische Infrastrukturen ist eine besonders wirksame Resilienzmaßnahme, weil sie bereits auf der Ebene der Exposition ansetzt. Wo kritische Anlagen nicht oder nur in vermindertem Maß gefährdenden Einwirkungen ausgesetzt sind, verringert sich regelmäßig auch der Bedarf an nachträglicher technischer Härtung und aufwändigen Kompensationsmaßnahmen. Die Standortfrage betrifft nicht nur die Wahl des Gesamtstandorts, sondern auch die Lage einzelner kritischer Anlagen und Infrastrukturelemente innerhalb eines bestehenden Standorts. Soweit eine vollständige Verlagerung nicht möglich oder nicht verhältnismäßig ist, ist zu prüfen, ob besonders empfindliche oder ausfallkritische Komponenten in weniger exponierte Gebäudeteile, Geschosse oder Anlagenbereiche verlegt werden können. Dies gilt insbesondere für Leit- und Schaltanlagen, Energie- und Notstromversorgung, Pumpen- und Medienversorgung, Kommunikations- und Steuerungseinrichtungen sowie sicherheitsrelevante Hilfssysteme.

Für die Beurteilung, ob ein Standort oder Anlagenbereich als hochgefährdet anzusehen ist, sind die relevanten Naturgefahren und standortbezogenen Einwirkungen systematisch zu berücksichtigen. Maßgeblich ist dabei nicht nur die formale Lage in ausgewiesenen Gefahrenzonen, sondern auch die konkret mögliche Exposition

gegenüber Überflutung, Rückstau, Auftrieb, Unterspülung, Hitze, Windlasten, Schnee- und Eislasten, mechanischen Einwirkungen oder eingeschränkter Erreichbarkeit. Ebenso zu berücksichtigen sind mögliche Kaskadeneffekte, wie etwa der gleichzeitige Ausfall von Zufahrten, Energieversorgung, Telekommunikation oder Hilfssystemen infolge eines äußeren Ereignisses.

Ist die Vermeidung eines hochgefährdeten Standorts nicht möglich, so erhöht sich der Bedarf an zusätzlichen Maßnahmen zur strukturellen Härtung und betrieblichen Vorsorge. Die Standortfrage ist daher nicht als einmalige Planungsentscheidung, sondern als grundlegender Bestandteil der Resilienzbewertung zu verstehen.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖNORM EN 1990	Eurocode – Grundlagen der Tragwerksplanung
ÖNORM B 1990-1	Eurocode – Grundlagen der Tragwerksplanung – Teil 1: Hochbau – Nationale Festlegungen zu ÖNORM EN 1990
OIB	Richtlinien des österreichischen Instituts für Bautechnik

Stand: 01. Juni 2026

Tipps

Gefahrenzonenpläne, Hochwasseranalysen, Raumordnungsunterlagen, Standortbewertungen und Versicherungsanalysen sollen systematisch ausgewertet werden. Nicht nur der Gesamtstandort, sondern auch die Lage kritischer Anlagen am Standort soll bewertet werden.
Wenn eine Verlagerung nicht möglich ist, sollen kompensierende Maßnahmen wie etwa erhöhte Aufstellung, Abdichtung, räumliche Trennung, mobile Schutzsysteme oder alternative Zugänge beschrieben werden.

3.2 Strukturelle und technische Härtung

Die strukturelle und technische Härtung umfasst Maßnahmen, die darauf gerichtet sind, kritische Infrastrukturen gegenüber äußeren Einwirkungen widerstandsfähiger zu machen. Dazu zählen z.B. Brandschutz, Schutz vor Überflutung, Sturm und Trockenheit sowie Flüssigkeitsdichtheit.

Die physische Systemintegrität – also jener Zustand, in dem Gebäude und Anlagen ihre Trag-, Schutz-, Dichtheits- und Funktionseigenschaften bewahren – ist eine grundlegende Voraussetzung für die Betriebsfähigkeit. Ohne physische Integrität ist weder ein sicherer Betrieb noch Notbetrieb noch geordneter Wiederanlauf in belastbarer Weise möglich.

Schutz vor Wasser-, Flüssigkeits- und Überflutungseinwirkungen

Wasser kann die physische Integrität in vielfacher Weise beeinträchtigen, etwa durch

Überflutung, Rückstau, Auftrieb, Unterspülung, Durchfeuchtung oder das Volllaufen tieferliegender Räume. Kritische Infrastrukturen sollen möglichst nicht in hochwasser- oder rückstaugefährdeten Bereichen platziert werden. Wo dies nicht möglich ist, sind Schutzmaßnahmen wie erhöhte Anordnung, bauliche Abschottung, Abdichtung, Rückstausicherung, Entwässerung oder druckwasserdichte Ausführung vorzusehen. Auch mittelbare Schäden wie auf Behälter einwirkende Auftriebskräfte, Unterspülung von Fundamenten, Kurzschlüsse und die Unterbrechung von Zugängen sind zu berücksichtigen.

Schutz gegen Wind-, Schnee-, Eis- und sonstige äußere Lasten
Windlasten können auf Gebäudehüllen, Dachkonstruktionen, freistehende technische Einrichtungen, Masten, Rohrleitungen und Kabeltrassen einwirken. Schnee- und Eislasten können die Tragfähigkeit von Dächern, Rohrbrücken und Einhausungen beeinträchtigen und durch Vereisung beweglicher Komponenten Funktionsstörungen verursachen. Resilienzmaßnahmen umfassen geeignete konstruktive Auslegung, verstärkte Befestigung, sichere Einhausung exponierter Bauteile und die Sicherstellung der Erreichbarkeit kritischer Bereiche auch unter außergewöhnlichen Witterungsbedingungen.

Schutz gegen thermische, Brand-, Druck- und Explosionswirkungen
Die Integrität von Gebäuden, Anlagen und technischen Infrastrukturen kann durch Brandbelastungen, Hitzewirkungen infolge angrenzender Schadenslagen sowie Druck- und Stoßbeanspruchungen aus Explosionen erheblich beeinträchtigt werden. Solche Einwirkungen können nicht nur einzelne Bauteile schädigen, sondern auf verbundene Systeme und Hilfsfunktionen (wie Energieversorgung, Kühlung, Mess- und Kommunikationstechnik oder Abschottungen) übergreifen.

Geeignete Maßnahmen umfassen erhöhte thermische Widerstandsfähigkeit von Bauteilen, brandschutztechnische Abschottung, geschützte Anordnung exponierter Infrastruktur sowie die Begrenzung von Folgeschäden durch bauliche und technische Vorkehrungen.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖNORM B 1990-x (Reihe)	Eurocode – Grundlagen der Tragwerksplanung
ÖNORM EN 1991-x (Reihe)	Eurocode – Grundlagen der Tragwerksplanung
OIB-Richtlinie 1	Mechanische Festigkeit und Standsicherheit
OIB-Richtlinie 2	Brandschutz
ÖNORM B 2501	Entwässerungsanlagen für Gebäude und Grundstücke – Planung, Ausführung und Prüfung

Stand: 01. Juni 2026

Tipps

Bauliche Schutzmaßnahmen sollen auf praktische Wirksamkeit geprüft werden. Türen, Abschottungen, Rückstauklappen oder mobile Elemente helfen nur, wenn sie funktionsfähig, bekannt und zugänglich sind und der Umgang mit diesen geübt ist. Indirekte Folgen wie Kurzschluss, Korrosion, Ausfall von Zugängen oder Verlust der Bedienbarkeit sollen in Hinblick auf die Auswirkungen auf den wesentlichen Dienst mitbetrachtet werden.
HORA (Natural Hazard Overview & Risk Assessment Austria) bietet eine frei zugängliche, kartenbasierte Erstbewertung standortbezogener Naturgefahren. HORA ersetzt keine vertiefende Gefahrenanalyse, gibt aber eine rasche Orientierung zur Exposition eines Standorts.

3.3 Nichtstrukturelle Maßnahmen und naturbasierte Lösungen

Neben baulichen und technischen Härtungsmaßnahmen erfordert die Katastrophenvorsorge auch nichtstrukturelle Maßnahmen, die darauf gerichtet sind, die Handlungsfähigkeit der kritischen Einrichtung unter Belastungsbedingungen zu sichern und die Wirksamkeit technischer Resilienzmaßnahmen durch organisatorische, betriebliche und personelle Vorkehrungen zu ergänzen. Kritische Einrichtungen haben ebenso nichtstrukturelle Maßnahmen zu treffen, etwa Training und Sicherheitsprotokolle.

Organisatorische Schutzmaßnahmen umfassen insbesondere die Festlegung von Zuständigkeiten, Entscheidungswegen, Alarmierungs- und Eskalationsmechanismen sowie die Zuordnung von Verantwortlichkeiten für Schutzhandlungen bei erkennbaren Belastungslagen. Fehlende oder unklare Zuständigkeiten können dazu führen, dass Schutzmaßnahmen verspätet ausgelöst oder unterlassen werden und dadurch technische Schutzwirkungen erheblich geschwächt werden.
Betriebliche Schutzmaßnahmen betreffen die konkrete Vorbereitung und Durchführung von Handlungen zur Sicherung von Anlagen und Infrastruktur gegen absehbare äußere Belastungen. Dies umfasst etwa die kontrollierte Außerbetriebnahme bestimmter Systeme, die Sicherung gefährdeter Bereiche, die Priorisierung kritischer Zugänge oder die temporäre Verlagerung gefährdeter Betriebsmittel. Solche Maßnahmen müssen auf die konkreten Risiken und die zeitlichen Anforderungen der jeweiligen Belastungslage abgestimmt sein.

Training und vorbereitete Handlungsabläufe stellen sicher, dass Beschäftigte und verantwortliche Funktionsträger bei äußeren Belastungslagen auf vorbereitete Vorgehensweisen zurückgreifen können. Vorbereitete Handlungsabläufe legen fest, welche Maßnahmen bei bestimmten Vorwarnlagen oder Schadensbildern einzuleiten sind, in welcher Reihenfolge dies zu geschehen hat und welche Stellen einzubinden sind. Von besonderer Bedeutung ist, dass Training und Handlungsabläufe nicht nur den Regelbetrieb, sondern ausdrücklich auch atypische und belastete Situationen erfassen.

Ergänzend können naturbasierte Lösungen zur Katastrophenvorsorge beitragen. Kritische Einrichtungen sollen naturbasierte Lösungen in Betracht ziehen, etwa die

Integration von Grüninfrastruktur wie renaturierten Feuchtgebieten zur Absorption von Sturmfluten oder urbanen Waldflächen zur Verringerung des Hitzeinsel-Effekts auf elektrische Anlagen. Naturbasierte Lösungen ergänzen technische und bauliche Maßnahmen, indem sie die Exposition gegenüber Extremereignissen verringern und die Widerstandsfähigkeit des Standortumfelds verbessern. Sie können insbesondere dort einen Beitrag leisten, wo konventionelle Härtungsmaßnahmen allein nicht ausreichen oder wo eine standortbezogene Risikominderung über die Gestaltung der unmittelbaren Umgebung erzielt werden kann.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖNORM EN ISO 22301	Sicherheit und Resilienz – Business Continuity – Management System – Anforderungen
ÖNORM EN ISO 22361	Sicherheit und Resilienz – Krisenmanagement – Leitlinien
ÖNORM S 2304	Integriertes Katastrophenmanagement - Benennungen und Definitionen

Stand: 01. Juni 2026

Tipps

Alarmpläne, Sicherheitsprotokolle, Wetterwarnprozesse, Schulungen, Betriebsanweisungen und Übungen sollen als nichtstrukturelle Schutzmaßnahmen genutzt werden.
Für Starkregen, Sturm, Hitze, Schneelast oder Hochwasser sollen klare Vorwarn- und Handlungsschwellen festgelegt werden.
Naturbasierte Lösungen wie Grünflächen, Versickerungsflächen, Verschattung oder Rückhalteräume sollen ergänzend geprüft werden.

4 Klimawandelanpassung

Kritische Einrichtungen haben nicht nur gegenwärtige Naturgefahren zu berücksichtigen, sondern auch jene langfristigen Veränderungen, die sich aus veränderten klimatischen Bedingungen ergeben und die Integrität, Funktionsfähigkeit und Betriebsbedingungen von kritischen Infrastrukturen schrittweise oder sprunghaft beeinträchtigen können. Kritische Einrichtungen sollen die langfristigen Verschiebungen von Klimamustern berücksichtigen, welche die Resilienz des Gesamtsystems im Lauf der Zeit negativ beeinflussen können, wie etwa Extremhitze, Hochwasser und Pegelanstieg von Gewässern.

Anders als punktuelle Extremereignisse wirken langfristige Klimaveränderungen häufig nicht in Form eines einmaligen Schadens, sondern durch eine allmähliche Veränderung von Belastungsprofilen, Umweltbedingungen und Betriebsgrenzen. Erhöhte thermi-

sche Belastungen können die Alterung von Baustoffen, Dichtungen, Isolierungen und elektrotechnischen Komponenten beschleunigen, die Kühlleistung mindern und die Funktionsgrenzen empfindlicher Anlagen näher an den Regelbetrieb heranführen. Veränderte Niederschlagsmuster können Entwässerungs- und Rückhaltesysteme häufiger überlasten und Überflutungsrisiken erhöhen. Längere Trockenperioden können Bodenbewegungen, Setzungen und Einschränkungen bei Betriebs- und Löschwasserversorgung begünstigen.

Eine kritische Infrastruktur kann unter heutigen Bedingungen noch ausreichend robust erscheinen und dennoch in ihrer Resilienz erheblich geschwächt werden, wenn sich Temperaturbereiche, Wasserverfügbarkeit, Feuchtebelastung oder externe Lastannahmen schrittweise verändern. Langfristige Klimaveränderungen können damit zu einer schleichenden Verringerung von Sicherheitsreserven und zu einer zunehmenden Empfindlichkeit gegenüber zusätzlichen Belastungen führen.

Von besonderer Bedeutung ist, dass sich verändernde klimatische Bedingungen nicht nur auf einzelne Komponenten auswirken, sondern auch auf das Zusammenspiel von Bauwerk, Technik, Hilfssystemen und Betriebsorganisation. Höhere Temperaturen können gleichzeitig Gebäude, elektrische Komponenten, Kühlung, Personalbelastung und Wasserbedarf beeinflussen. Wiederkehrende Überflutungs- oder Feuchteereignisse können nicht nur bauliche Schäden verursachen, sondern auch Korrosion, Funktionsverluste und Verzögerungen bei Wiederherstellung nach sich ziehen.

Wasser ist in vielen kritischen Einrichtungen eine grundlegende Voraussetzung für technische Prozesse, Kühlung, Reinigung, Dampf- oder Medienerzeugung, Brandschutz oder sonstige betriebsnotwendige Funktionen. Kritische Einrichtungen sollen Maßnahmen gegen Wasserknappheit planen. Dies erfordert eine systematische Analyse der wasserbezogenen Abhängigkeiten der Einrichtung. Zu betrachten ist insbesondere, welche Prozesse und technischen Systeme auf Wasser angewiesen sind, welche Mindestmengen für sicheren Betrieb und Notbetrieb erforderlich sind und in welchem Maß alternative Quellen, Speicher oder Rückfalllösungen verfügbar sind. Wasserknappheit darf dabei nicht isoliert betrachtet werden; sie kann sich mit Hitzeperioden, erhöhter Kühlanforderung und eingeschränkter Löschwasserversorgung überlagern.

Kritische Einrichtungen sollen durch Stresstests sicherstellen, dass sie in einer signifikant wärmeren oder feuchteren Umgebung funktionsfähig bleiben. Ein Stresstest untersucht, wie sich extreme oder veränderte Umweltbedingungen auf kritische Funktionen, Prozesse und Assets auswirken und ob die bestehenden Schutzmaßnahmen ausreichend sind. Dies kann sich etwa auf langanhaltende Hitzeperioden, gleichzeitige Stromversorgungs- und Kühlungsprobleme, außergewöhnliche Niederschlagsmengen, Wasserknappheit oder Ketteneffekte in Hinblick auf Versorgung und die Verfügbarkeit von Personal beziehen. Stresstests können technisch, organisatorisch oder kombiniert ausgestaltet sein und auf Modellierungen, Szenarien, Übungen oder interdisziplinären Bewertungen beruhen. Entscheidend ist, dass sie die Frage beantworten, ob die kritische Einrichtung unter plausibel verschärften Umweltbedingungen die Erbringung des wesentlichen Dienstes noch aufrechterhalten kann.

Kritische Einrichtungen haben langfristige Veränderungen der klimatischen Bedingungen systematisch in ihre Bewertung physischer Systemintegrität einzubeziehen. Zu prüfen ist, ob bestehende Schutzmaßnahmen auch unter künftig veränderten Umweltbedingungen noch ausreichend wirksam sind, welche Strukturen oder Systeme besonders empfindlich auf schleichende Belastungsänderungen reagieren und an welchen Stellen Anpassungen erforderlich werden.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖNORM EN 1991-x (Reihe)	Eurocode – Grundlagen der Tragwerksplanung
ÖNORM EN ISO 14090	Anpassung an den Klimawandel – Grundsätze, Anforderungen und Leitlinien
ÖNORM EN ISO 14091	Anpassung an den Klimawandel – Vulnerabilität, Auswirkungen und Risikobewertung

Stand: 01. Juni 2026

Tipps

Bestehende Auslegungsannahmen sollen auf künftige Bedingungen überprüft werden, etwa Kühlreserven, Löschwasserverfügbarkeit, Entwässerungskapazität, Materialalterung oder Arbeitsbedingungen.
Zu prüfen ist, welche Anlagen, Prozesse und Hilfssysteme durch Hitze, Starkregen, Trockenheit, Feuchte, Wasserknappheit oder Sturm anfälliger werden.
Stresstests sollen konkrete Belastungslagen abbilden, etwa länger anhaltende Hitze, Starkregen mit Rückstau, Wasserknappheit oder gleichzeitige Strom- und Kühlungsprobleme.

5 Ereigniserfassung und Incident Learning

Die Einrichtung einer Datenbank für relevante Ereignisse und die Umsetzung eines systematischen Ereignismeldesystems schaffen eine Ereignishistorie, die nicht nur die Prävention von Vorfällen und Risikominderung ermöglicht, sondern auch die Wiederherstellung von Anlagen und Betriebsmitteln unterstützt.

Zu erfassen sind somit nicht nur Sicherheitsvorfälle mit sichtbaren Auswirkungen, sondern auch Störungen und Beinahe-Sicherheitsvorfälle mit Erkenntniswert für die Resilienz. Gerade kleinere Störungen oder Beinahe-Sicherheitsvorfälle können auf Schwachstellen hinweisen, bevor es zu einer erheblichen Störung oder dem Ausfall des wesentlichen Dienstes kommt. Erfasst werden sollen insbesondere technische Fehlfunktionen, Auslösungen von Schutzsystemen, Überlastungen oder unplausible Betriebszustände, temporäre Ausfälle kritischer Funktionen, Bedienfehler oder Fehlalarme mit systemischem Erkenntniswert, Kommunikations- oder Zugangsproble-

me sowie signifikante Abweichungen von Standardverfahren. Ebenso einzubeziehen sind Situationen, in denen schwerwiegende Folgen nur durch Zufall oder besonders günstige Randbedingungen ausgeblieben sind. Diese Meldekriterien sollen eindeutig, praktikabel und bereichsübergreifend vergleichbar sein. Gleichzeitig ist darauf zu achten, dass das Reporting nicht durch übermäßige Formalisierung oder Angst vor Sanktionen behindert wird. Eine resilienzorientierte Meldekultur setzt voraus, dass sicherheitsrelevante Beobachtungen verlässlich gemeldet werden können, ohne dass jede Meldung als persönliches Fehlverhalten interpretiert wird.

Die dokumentierten Ereignisdaten sollen so strukturiert sein, dass sie für Ursachenanalyse, Maßnahmenbewertung und kontinuierliche Verbesserung genutzt werden können. Die Dokumentation sollte zumindest Ereignistyp, Zeitpunkt, betroffene Funktionen oder Assets, Art der Beeinträchtigung, vermutete oder bestätigte Ursachen, ergriffene Sofortmaßnahmen, Auswirkungen auf die Erbringung des wesentlichen Dienstes, Wiederherstellungsmaßnahmen, Wiederanlaufzeiten sowie abgeleitete Verbesserungsmaßnahmen umfassen.

Die Ereigniserfassung entfaltet ihren Nutzen erst durch systematische Auswertung. Ziel ist es, Muster, Häufungen, strukturelle Schwächen, wiederkehrende Ausfallursachen und Verbesserungspotenziale zu erkennen. Die Auswertung sollte insbesondere klären, welche Ursachen oder Schwachstellen wiederholt auftreten, welche kritischen Funktionen besonders betroffen sind, ob bestehende Maßnahmen tatsächlich wirksam waren und welche Anpassungen im Resilienzplan daraus abzuleiten sind. Erkannte Verbesserungsmaßnahmen sind zu priorisieren, den verantwortlichen Stellen zuzuweisen und in ihrer Umsetzung systematisch nachzuverfolgen.

Über die reine Prävention hinaus dient die systematische Erfassung der Ereignisse auch der Steuerung der Wiederherstellung von Anlagen und Betriebsmitteln. Strukturiert erfasste Informationen über Schadensverläufe, betroffene Komponenten, Wiederanlaufzeiten und wirksame Wiederherstellungsmaßnahmen ermöglichen es, bei künftigen Vorfällen schneller und gezielter zu reagieren.

Die Ergebnisse der Auswertung sollen regelmäßig in die Überprüfung von Schutzzielen, Maßnahmen, Übungen, Schulungen und Wiederanlaufregelungen einfließen. So entsteht ein geschlossener Lernkreislauf zwischen Ereigniserfahrung, Maßnahmenanpassung und Weiterentwicklung des Resilienzsystems.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖNORM EN ISO 9001	Qualitätsmanagementsysteme – Anforderungen
ÖNORM EN ISO 22301	Sicherheit und Resilienz – Business Continuity – Management System – Anforderungen
DIN ISO 22320	Sicherheit und Resilienz – Gefahrenabwehr – Leitfaden für die Organisation der Gefahrenabwehr bei Schadensereignissen
ÖNORM ISO 31000	Risikomanagement – Leitlinien
API RP 754	Process Safety Performance Indicators for the Refining and Petrochemical Industries
OVE EN IEC 62682	Alarmmanagement in der Prozessindustrie

Stand: 01. Juni 2026

Tipps

Bestehende Systeme für Unfallmeldungen, Störungsmeldungen, Auditfeststellungen, Instandhaltungsmeldungen und Lessons Learned können genutzt und um Resilienzaspekte ergänzt werden.
Erfasst werden sollen auch Ereignisse ohne Schaden, wenn sie Hinweise auf Schwachstellen, kritische Abhängigkeiten oder mögliche Ausfälle des wesentlichen Dienstes geben.
Ereignisdaten sollen ausgewertet und in die Überarbeitung von Betriebsanweisungen, Prüfpläne, Schulungen, Übungen und das Gesamtkonzept integriert werden.

6 Prävention menschlicher Fehler

Zur Prävention menschlicher Fehler sollen kritische Einrichtungen fehleranfällige Tätigkeiten identifizieren und geeignete Gegenmaßnahmen einsetzen. Darunter fallen etwa Automatisierung, kontinuierliche Schulung, Mitarbeiteraufsicht und -verantwortlichkeit, detaillierte Prozessdokumentation, regelmäßige Audits und Inspektionen sowie die Entwicklung einer Kultur der Resilienz und Verantwortung.

Am Beginn steht die Identifikation jener Tätigkeiten, Prozesse und Handlungssituationen, bei denen menschliche Fehler besonders wahrscheinlich sind oder erhebliche Auswirkungen auf den wesentlichen Dienst haben können. Fehleranfällige Tätigkeiten können insbesondere sicherheitsrelevante Bedienhandlungen, Schalt- und Freigabevorgänge, manuelle Eingriffe in automatisierte Prozesse, In- und Außerbetriebnahmen, Wartungs- und Instandhaltungstätigkeiten, Notfallmaßnahmen sowie Arbeiten unter Zeitdruck sein. Besonders kritisch sind Situationen, in denen mehrere Belastungsfaktoren zusammentreffen (wie etwa Zeitdruck, unvollständige Information, Personalmangel oder komplexe technische Schnittstellen), weil dadurch die Wahrscheinlich-

keit von Fehlhandlungen steigt und die Möglichkeiten zur rechtzeitigen Fehlerkorrektur eingeschränkt sind. Die Bewertung soll Betriebserfahrung, Beinahe-Sicherheitsvorfälle, Auditergebnisse und Rückmeldungen des Personals einbeziehen.

Schulung und Unterweisung müssen sich auf jene Tätigkeiten konzentrieren, die für den sicheren Betrieb, den Notbetrieb, die Wiederaufnahme oder Wiederherstellung besonders relevant sind. Schulungen sollen nicht nur allgemeines Sicherheitswissen vermitteln, sondern konkrete Handlungsfähigkeit herstellen. Dazu zählen insbesondere die Kenntnis kritischer Prozesse und Zuständigkeiten, die sichere Anwendung von Standardverfahren, das Verhalten bei Abweichungen und Warnlagen, die Einhaltung von Eskalations- und Meldewegen sowie die Anwendung manueller Ersatzverfahren.
Prozessdisziplin bedeutet, dass sicherheitsrelevante Abläufe nachvollziehbar dokumentiert, konsequent eingehalten, regelmäßig überprüft und bei Bedarf angepasst werden. Dies umfasst insbesondere klare Arbeitsanweisungen, Checklisten, Vier-Augen-Prinzipien, Freigaberegeln, definierte Kontrollpunkte sowie regelmäßige Audits und Inspektionen.

Automatisierung und technische Kontrollmechanismen können menschliche Fehler deutlich reduzieren. Sie sind dort sinnvoll, wo sie Fehlbedienungen verhindern, kritische Zustände anzeigen, Plausibilitätsprüfungen ermöglichen oder Bedienhandlungen absichern. Gleichzeitig muss festgelegt sein, wie bei Ausfall oder Fehlfunktion solcher Systeme gehandelt wird.

Wirksame personelle Resilienz setzt klare Verantwortlichkeiten voraus. Für kritische Tätigkeiten muss festgelegt sein, wer entscheidet, wer ausführt, wer kontrolliert und wer bei Abweichungen eingreift. Mitarbeiteraufsicht dient nicht primär der Sanktionierung, sondern der Sicherstellung verlässlicher Abläufe. Eine Resilienzkultur unterstützt diese Zielsetzung, indem sie Sicherheitsbewusstsein, Meldebereitschaft, Verantwortungsübernahme und einen offenen Umgang mit Fehlern und Beinahe-Sicherheitsvorfällen fördert. Beschäftigte sollen sicherheitsrelevante Beobachtungen ansprechen und melden können, ohne dass jede Meldung automatisch als individuelles Fehlverhalten verstanden wird. Führungskräfte sollen sicherheitsgerechtes Verhalten aktiv unterstützen.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖNORM EN ISO 9001	Qualitätsmanagementsysteme – Anforderungen
ÖNORM ISO 45001	Managementsysteme für Sicherheit und Gesundheit bei der Arbeit – Anforderungen mit Anleitung zur Anwendung
ÖNORM EN ISO 6385	Grundsätze der Ergonomie für die Gestaltung von Arbeitssystemen
OVE EN 61882 (IEC 61882)	HAZOP-Verfahren (HAZOP-Studien) – Anwendungsleitfaden
OVE EN 61511-x (Reihe)	Functional safety – Safety instrumented systems for the process industry sector
OVE EN IEC 62682	Alarmmanagement in der Prozessindustrie

Stand: 01. Juni 2026

Tipps

Schulungen, Unterweisungen, die Anwendung des Vier-Augen-Prinzips, Checklisten, Freigabeverfahren und Audits sollen gezielt auf kritische Tätigkeiten ausgerichtet werden. Automatisierung kann Fehler reduzieren, muss aber durch klare Rückfallebenen ergänzt werden.
Schulungen sollen sicheres Handeln unter Zeitdruck, unvollständiger Information und abweichenden Betriebszuständen trainieren.

7 Abschließende Vorgaben

Für die Umsetzung des Leitfadens Z 1 wird nochmals darauf hingewiesen, dass sämtliche Anforderungen auf den wesentlichen Dienst der kritischen Einrichtung bezogen sind. Die Resilienzmaßnahmen gemäß § 15 RKEG dienen nicht dem allgemeinen Schutz der Einrichtung als Unternehmen, sondern der Aufrechterhaltung der Fähigkeit, den wesentlichen Dienst zu erbringen. Ebenso sind die Grundsätze der Geeignetheit und Verhältnismäßigkeit, der Konformitätsvermutung einschließlich der Begründung bei Abweichungen, des Verhältnisses zu Normen und Richtlinien sowie der Stufenlogik der behördlichen Prüfung, wie in Leitfaden Z 0 dargelegt, zu beachten. Dem risikobasierten Ansatz folgend liegt die konkrete Ausgestaltung bei der kritischen Einrichtung selbst.

Die Präventions- und Schutzfunktion der vorgesehenen Maßnahmen soll dauerhaft aufrechterhalten werden. Übungen sind ein wesentliches Mittel, um die Wirksamkeit präventiver Maßnahmen zu überprüfen und sicherzustellen, dass das Personal seine Aufgaben im Ernstfall wirksam wahrnehmen kann. Dabei sollen kritische Einrichtungen den Fokus auf die Ergebnisse ihrer einrichtungsinternen Risikoanalyse legen und den vollständigen Präventionskreislauf testen. Ebenso soll die Zusammenarbeit mit einschlägigen Behörden und Einsatzorganisationen sichergestellt und diese in Übungen einbezogen werden. Soweit Wartungen, Überprüfungen, Aktualisierungen oder sonstige wiederkehrende Maßnahmen erforderlich sind, sollen diese verbindlich vorgesehen und nachvollziehbar dokumentiert werden.

Z 2: Physischer Schutz

In Kooperation mit VSÖ VERBAND DER SICHERHEITSUNTERNEHMEN ÖSTERREICHS

1 Allgemeine Grundlagen

Kritische Einrichtungen haben geeignete und verhältnismäßige Resilienzmaßnahmen zu treffen, um die physische Infrastruktur zur Erbringung ihrer wesentlichen Dienste gegenüber natürlichen Gefahren und menschengemachten Bedrohungen zu schützen und ihre Funktionsfähigkeit aufrechtzuerhalten.

Bei der Planung von Resilienzmaßnahmen haben kritische Einrichtungen die Relevanz spezifischer Bedrohungsszenarien zu berücksichtigen. Insbesondere ist Folgendes zu beachten:

Unter Berücksichtigung der Notwendigkeit einer engen öffentlich-privaten Zusammenarbeit mit den zuständigen Behörden ist ein angemessener und wechselseitiger Austausch sicherheitsrelevanter Informationen sicherzustellen, um die Entwicklung und Aufrechterhaltung eines gemeinsamen Lagebildes zu ermöglichen. Hierzu zählt insbesondere eine Abstimmung in Bezug auf relevante Bedrohungsszenarien und zugehörige Eintrittswahrscheinlichkeiten mit den Expertinnen und Experten aus dem BMI und anderen Ministerien als wesentlicher Bestandteil von Security-Risikoanalysen der Sektoren bzw. Unternehmen.

Im Falle potenzieller hybrider Bedrohungen durch ausländische Akteure, die sich etwa in Sabotagehandlungen zur Störung von kritischen Infrastrukturen oder in entsprechenden Vorbereitungshandlungen, einschließlich Spionage- oder Aufklärungsmaßnahmen, äußern können, ist insbesondere zu berücksichtigen:

1. dass staatliche Akteure verwundbare oder beeinflussbare Dritte („Proxies") – etwa Einzelpersonen oder Gruppen – finanzieren, unterstützen oder steuern können, um ihre Ziele zu erreichen;
2. dass staatliche Akteure koordinierte Angriffe über mehrere Angriffsvektoren und/oder unter Einsatz mehrerer Proxies durchführen können.

Darüber hinaus sind potenzielle Bedrohungen durch Terrorismus und gewaltbereiten Extremismus, kriminelle Handlungen, militärische Angriffe oder gezielte militärische Zielansteuerung im Konflikt- oder Kriegsfall, Insider-Bedrohungen, aktivistische Handlungen sowie Spionage und Sabotage als weitere vorsätzliche Bedrohungen zu berücksichtigen.

Die Resilienzmaßnahmen der physischen Sicherheit sollen darauf ausgerichtet sein, Angriffe präventiv zu verhindern, sicherheitsrelevante Ereignisse frühzeitig zu erkennen, deren Fortschreiten zu verzögern oder zu verhindern, eine wirksame Reaktion zu ermöglichen und die Auswirkungen von Vorfällen zu minimieren.

Eine risikobasierte Vorgehensweise in der physischen Sicherheit setzt die Identifikation relevanter Schutzgüter voraus. Bei der Festlegung der Schutzziele soll sichergestellt sein, dass diese all jene Schutzgüter absichern, die unmittelbar oder mittelbar für die Erbringung des wesentlichen Dienstes relevant sind. Als Orientierungsrahmen dienen die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit.

Risiken sollen unter Verwendung geeigneter und hinreichend granularer Szenarienkataloge zunächst identifiziert und anschließend analysiert sowie hinsichtlich ihrer Eintrittswahrscheinlichkeit und Auswirkungen bewertet werden, um daraus angemessene Resilienzmaßnahmen abzuleiten. Für die Ermittlung der Eintrittswahrscheinlichkeit empfiehlt es sich, die aktuelle Bedrohungslage sowie die Verwundbarkeit der jeweiligen Schutzgüter als bestimmende Faktoren zu berücksichtigen.

Die Ermittlung und Bewertung der Risiken soll durch eine Analyse aus der Perspektive potenzieller Angreifer ergänzt werden, in deren Rahmen die relevanten Angriffsvektoren objektivierbar und nachvollziehbar darzulegen sind. Als Angriffsvektoren gelten dabei jene Wege und Methoden, über die ein Angreifer im Sinne einer Schutzzielverletzung auf ein Schutzgut einwirken kann.

Zur fundierten Ableitung eines in sich abgestimmten Schutzkonzepts soll entlang der identifizierten Angriffsvektoren eine Schichtenanalyse durchgeführt werden, die sich von der äußersten Schutzschicht bis zum Schutzgut erstreckt. Zu untersuchen ist, welche Schutzschichten ein Angreifer überwinden müsste, um das Schutzgut zu erreichen; jede Schicht ist dabei hinsichtlich ihrer Wirksamkeit und möglicher Schwachstellen zu bewerten.

In die Betrachtung sind technische, organisatorische und personelle Maßnahmen der Verhinderung, der Erkennung, der Verzögerung sowie der Reaktion und Wiederaufnahme einzubeziehen. Auf dieser Grundlage lässt sich die Verwundbarkeit der Schutzgüter systematisch ableiten, bewerten und durch geeignete Resilienzmaßnahmen gezielt verringern. Insbesondere sollen geeignete und verhältnismäßige Mechanismen zur Detektion und Alarmierung vorgesehen, eine dem jeweiligen Risiko entsprechende physische Widerstandszeit gewährleistet sowie eine koordinierte Intervention durch geeignete Interventionskräfte sichergestellt werden.

Bei der Auslegung des Schutzkonzepts ist sicherzustellen, dass die Zeit, die zur Durchführung eines Angriffs auf ein Schutzgut benötigt wird, größer ist als die Reaktionszeit des physischen Schutzsystems. Die Reaktionszeit umfasst dabei die Zeitspannen für die Detektion und Verifikation eines sicherheitsrelevanten Ereignisses, die Alarmierung der zuständigen Interventionskräfte sowie deren Anreise zum Angriffsort, um den Angriff vor Erreichen des Angriffszieles zu stoppen. Die physischen Barrieren entlang des Angriffspfades sollen daher über eine ausreichende Widerstandszeit verfügen, um einen Angriff so lange zu verzögern, dass die Interventionskräfte vor Erreichen des Angriffszieles wirksam eingreifen können. Die Reaktionszeit ist im Schutzkonzept zu dokumentieren; die Interventionszeit ist mit den zuständigen Interventionskräften abzustimmen.

Die Intervention kann, abhängig von Schutzziel, Täterqualität und örtlichen Gegebenheiten, durch die örtlich zuständigen Exekutivkräfte, durch internes Sicherheitspersonal, durch externe zertifizierte Interventionsdienste oder durch Kombinationen dieser Varianten erfolgen.

Die Planung, Umsetzung, laufende Steuerung und Verbesserung von Resilienzmaßnahmen müssen anhand einer nachvollziehbaren und in Bezug auf die ermittelten Schutzgüter sowie festgelegten Bedrohungsszenarien schlüssigen Dokumentation erfolgen, so dass eine behördliche Überprüfung hinsichtlich der risikobezogenen Angemessenheit und Wirksamkeit der Resilienzmaßnahmen durchführbar ist. Zugleich kann diese Dokumentation der kritischen Einrichtung als nützliches und integriertes Steuerungs- und Entscheidungsinstrument dienen und damit zu einem effektiven und nachhaltigen Schutz des wesentlichen Dienstes gegen natürliche oder menschengemachte Bedrohungen beitragen.

Sämtliche Einrichtungen und Ausrüstungen, die in relevantem Zusammenhang mit den wesentlichen Diensten stehen, jedoch auf Liegenschaften Dritter untergebracht sind, sollen gleichermaßen angemessenen Schutzmaßnahmen unterliegen.

Vernetzend mit der NIS-2-Richtlinie ist festzuhalten, dass die für die Erbringung des wesentlichen Dienstes unmittelbar oder mittelbar relevanten physischen Träger von Informationen gleichsam dem Bereich der relevanten physischen Infrastruktur zuzuordnen sind. Dies bedeutet unter anderem, dass diese Schutzgüter im Sinne des vorliegenden Leitfadens Z 2 in Bezug auf den wesentlichen Dienst ebenfalls zu behandeln und zu schützen sind.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖNORM S 2412	Security Management System – Benennungen und Definitionen
ÖNORM S 2413	Security Management System – Grundlagen und Prozesse
ÖNORM S 2414-2	Security Management System – Teil 2: Leitfaden für die Einbettung der physischen Sicherheit in das Security Management System
ÖNORM S 2415-1	Security Management System – Teil 1: Anforderungen an ein Security Management System
ÖNORM S 2415-2	Security Management System – Teil 2: Anforderungen an die Qualifikation eines Security Managers

Stand: 01. Juni 2026

2 Bauliche und mechanische Maßnahmen

Bauliche und mechanische Maßnahmen dienen der Herstellung und Aufrechterhaltung physischer Barrieren und Widerstände im Bereich von Liegenschaftsgrenzen und sonstigen Umfassungsbauwerken, der Gebäudeaußenhülle sowie von geschützten Räumen bzw. Zonen innerhalb von Gebäuden. Sie definieren und markieren räumliche Abgrenzungen zwischen unterschiedlichen Sicherheitsbereichen und tragen – entsprechend dem jeweiligen Schutzbedarf – durch physische Widerstandswerte zur Verzögerung

von Angriffen und damit zur Erhöhung der Widerstandszeit bei und sollen von außen nach innen konzipiert werden.

Baulich-mechanische Sicherheitsmaßnahmen betreffen insbesondere öffenbare oder bewegliche Elemente der Liegenschafts- und Bauwerksumfassung sowie innerhalb geschützter Räume bzw. Zonen, wie etwa Zäune, Zufahrts- und Zugangstore, Türen, Fenster, Oberlichten oder Lichtkuppeln. Sie umfassen darüber hinaus Schutzbehältnisse, insbesondere Wertschutzbehältnisse, soweit diese dem Schutz relevanter Schutzgüter dienen.

2.1 Perimeter und Freigelände

Der Perimeter relevanter Liegenschaften soll eine klare, durchgehende Verteidigungslinie bilden und über seine gesamte Ausdehnung ein gleichwertiges Schutzniveau gewährleisten. Identifizierte Schwachstellen oder Unterbrechungen im Perimeterschutz müssen im Rahmen der einrichtungsinternen Risikoanalyse bewertet werden.

Perimeteranlagen sollen entsprechend dem jeweiligen Risiko strukturell gehärtet und basierend auf der Riskoanalyse gegen typische Angriffsformen – insbesondere Durchdringen, Übersteigen, Unterkriechen sowie Untergraben – wirksam abgesichert werden. Der Zugang von Fahrzeugen, Personal und Gütern zu relevanten Liegenschaften ist über eine begrenzte Anzahl kontrollierbarer Kontrollpunkte zu führen.

Geeignete Beschilderungs- und Beleuchtungsmaßnahmen sollen ergänzend zur Abschreckung potenzieller Angreifer, zur Verbesserung der Überwachungswirkung sowie zur Vermeidung von toten Winkeln beitragen. Dabei ist zu berücksichtigen, dass sichtbare Sicherheitsmaßnahmen allgemein stets auch Aufmerksamkeit auf die Liegenschaft lenken können – bei kritischen Infrastrukturen, deren kritische Funktion nach außen nicht erkennbar ist, ist dieser Aspekt entsprechend bei der Wahl und Ausgestaltung solcher Maßnahmen miteinzubeziehen.

Besonderheit: Schutz vor Angriffen mit Fahrzeugen

Perimeteranlagen sollen entsprechend dem jeweiligen Risiko so ausgelegt werden, dass sie einen wirksamen Beitrag zum Schutz vor Angriffen unter Einsatz von Fahrzeugen leisten. Bei der Planung geeigneter und verhältnismäßiger Schutzmaßnahmen sind insbesondere das Freigelände, potenzielle Annäherungsräume sowie Anfahrtswege zu kritischen Infrastrukturen systematisch zu berücksichtigen.

Direkte Fahrzeugzufahrtsrouten sollen entsprechend dem jeweiligen Risiko durch eine geeignete Kombination physischer Barrieren eingeschränkt werden. Dazu zählen beispielsweise feste oder versenkbare Poller, natürliche Hindernisse sowie sonstige Maßnahmen zur Geschwindigkeitskontrolle wie eine geeignete Verkehrs- oder Wegeführung. Bei der Auslegung ist der für das jeweilige Schutzziel erforderliche maximale Abstand zwischen benachbarten Barrieren einzuhalten, um ein Eindringen/Durchbrechen von Fahrzeugen wirksam zu verhindern.

Während statische Barrieren einen dauerhaften physischen Widerstand ohne kontrollierten Fahrzeugdurchlass bieten, ermöglichen dynamische Systeme einen gesteuerten und protokollierbaren Zugang für befugtes Personal und Lieferverkehr.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
VdS 3143	Sicherungsleitfaden Perimeter
DIN ISO 22343-1	Sicherheit und Resilienz – Fahrzeugsicherheitsbarrieren – Teil 1: Leistungsanforderung, Fahrzeuganprallprüfverfahren und Leistungsbewertung
DIN ISO 22343-2	Sicherheit und Resilienz – Fahrzeugsicherheitsbarrieren – Teil 2: Anwendung
DIN SPEC 91414-1	Mobile Fahrzeugsicherheitsbarrieren für Sicherheitsanforderungen – Teil 1: Anforderungen, Prüfmethoden und Leistungskriterien

Stand: 01. Juni 2026

Tipps

Kritische Einrichtungen verfügen häufig über weitläufige Außengrenzen oder eine Vielzahl an Liegenschaften, wodurch die Errichtung durchgehender baulicher Perimeteranlagen mit erheblichem finanziellem Aufwand verbunden sein kann.
In diesem Zusammenhang ist es wesentlich, die konkrete Funktion der Perimeteranlage im Schutzkonzept klar zu definieren: Die Notwendigkeit eines Perimeterschutzes ist immer im Gesamtkontext zu sehen und eine Perimeteranlage muss nicht zwingend einen hohen physischen Widerstand gegen Angriffe aufweisen. Ihre Kernaufgabe kann beispielsweise auch darin bestehen, eine physische Barriere als Grundlage für nachgelagerte Detektionsmaßnahmen zu schaffen.
Entscheidend ist dabei, dass ein unbefugtes Übertreten der Liegenschaftsgrenze nur mit erkennbarem Aufwand möglich ist und damit eindeutig als sicherheitsrelevantes Ereignis gewertet werden kann.

2.2 Gebäude

Zugangspunkte zu relevanten Gebäuden sowie geschützten Räumen und Zonen – wie etwa Tore, Türen, Fenster, Oberlichter oder Lichtkuppeln – sollen durch geeignete mechanische Verschlüsse so abgesichert werden, dass möglichen Angriffen in Summe ein dem Risiko angemessener physischer Widerstand entgegengesetzt wird.

Die den mechanischen Verschlüssen zugehörigen Rahmen- und Verankerungssysteme sowie die Bausubstanz relevanter Umfassungsbauwerke, Gebäudeaußenhüllen und geschützter Räume und Zonen sollen dabei keine Schwachstellen in Bezug auf den definierten physischen Widerstand darstellen.

Mögliche unkonventionelle Zugangspunkte, wie etwa Dachluken, Einstiegsschächte oder -rohre oder Lüftungsöffnungen sind dabei ebenso zu beachten und angemessen zu sichern.

Bei Bestandselementen sollen dem Risiko entsprechend geeignete Schutzvorkehrungen – wie etwa Verriegelungssysteme, Gitterstäbe, Schutzgitter, einbruchshemmendes Glas, Sicherheitsfolien oder vergleichbare Schutzschichten – vorgesehen werden.

Im Rahmen einer spezifischen Risikoanalyse ist zudem zu evaluieren, ob für die Aufrechterhaltung der wesentlichen Dienste mechanische Verschlüsse und Fassadenelemente gegen Beschuss und Sprengwirkung gesichert werden müssen.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖNORM EN 1627	Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse – Einbruchhemmung – Anforderungen und Klassifizierung
ÖNORM EN 356	Glas im Bauwesen – Sicherheitssonderverglasung – Prüfverfahren und Klasseneinteilung des Widerstandes gegen manuellen Angriff
ÖNORM B 5338	Einbruchhemmende Fenster, Türen und zusätzliche Abschlüsse – Allgemeine Festlegungen – Ergänzende Bestimmungen zu ÖNORM EN 1627
ÖNORM B 5351	Einbruchhemmende Baubeschläge – Schlösser, Schließbleche, Schutzbeschläge, Schließzylinder und Nachrüstprodukte für Fenster und Türen – Maße, Ausführung, Prüfung und Kennzeichnung
ÖNORM EN 1063	Glas im Bauwesen – Sicherheitssonderverglasung – Prüfverfahren und Klasseneinteilung für den Widerstand gegen Beschuss
ÖNORM EN 1522	Fenster, Türen, Abschlüsse – Durchschusshemmung – Anforderungen und Klassifizierung
ÖNORM EN 13123-1	Fenster, Türen, Abschlüsse und Vorhangfassaden – Sprengwirkungshemmung – Anforderungen und Klassifizierung – Teil 1: Stoßrohr
ÖNORM EN 13123-2	Fenster, Türen, Abschlüsse und Vorhangfassaden – Sprengwirkungshemmung - Anforderungen und Klassifizierung – Teil 2: Freilandversuch
ÖNORM EN 13541	Glas im Bauwesen – Sicherheitssonderverglasung – Prüfverfahren und Klasseneinteilung des Widerstandes gegen Sprengwirkung
VPAM	Prüfrichtlinien der Vereinigung der Prüfstellen für angriffshemmende Materialien und Konstruktionen

Stand: 01. Juni 2026

Tipps und Tricks

Bei der Planung mechanischer Bauteile sind frühzeitig alle zusätzlichen funktionalen Anforderungen zu berücksichtigen. Dazu zählt insbesondere der gleichzeitige Einsatz als Fluchttür oder Notausgang gemäß den Vorgaben des ArbeitnehmerInnenschutzes.
Daraus kann sich etwa die Notwendigkeit geeigneter Fluchtweg-, Notausgangs- oder Paniktürbeschläge sowie entsprechender mechanischer Verriegelungslösungen an der Innenseite ergeben.
Darüber hinaus sind bei Bauteilen im Außenbereich die Exposition gegenüber Temperaturschwankungen und Witterungseinflüssen zu berücksichtigen, sodass alle Funktionen unter den gegebenen Umgebungsbedingungen dauerhaft gewährleistet und die Bauteile uneingeschränkt nutzbar bleiben.
Bauteile der Widerstandsklassen RC5 und RC6 sind sowohl kostenseitig als auch in der praktischen Handhabung – insbesondere hinsichtlich Gewicht, Instandhaltung und Funktionserhaltung – mit erheblichem Aufwand verbunden. Die erforderliche physische Widerstandszeit kann alternativ durch die Reihenschaltung mehrerer Bauteile niedrigerer Widerstandsklassen bis maximal RC4 erreicht werden.
Vorhandene Zugangspunkte, die betrieblich keine relevante Funktion erfüllen, können baulich verschlossen oder durch geeignete bauliche Maßnahmen so verkleinert werden, dass eine Durchstiegsmöglichkeit ausgeschlossen wird. Auf diese Weise kann an den betroffenen Punkten der Bedarf an mechanischen Verschlusselementen samt der damit verbundenen Anschaffungs-, Errichtungs- und Wartungskosten entfallen.

2.3 Wertschutzschränke

Wertschutzschränke dienen dem Schutz von physischen Informationswerten, Datenträgern oder sonstigen Werten vor unbefugtem Zugriff. Sie sollen so ausgeführt und gesichert sein, dass der mechanische Widerstand angemessen in Bezug zum Schutzbedarf der darin befindlichen Schutzgüter ist sowie den anerkannten Zertifizierungen entspricht.

Bei der Aufstellung der Schränke sind bauliche Gegebenheiten, insbesondere die zulässige Decken- und Bodenbelastung, zu beachten. Schränke mit einem Eigengewicht unter 1000 kg müssen fachgerecht verankert werden, um ein Entfernen oder Umkippen zu verhindern.

Zusätzlicher Schutz gegen Feuer, Hitze, Feuchtigkeit oder andere Umwelteinflüsse ist primär über den Bereich oder Raum sicherzustellen, in dem der Schrank steht, da Wertschutzschränke nach den einschlägigen Normen selbst nicht zwingend feuerfest sind. Schutzschränke sind so zu verwalten, dass die Zugriffscodes und Berechtigungen jederzeit sicher und nachvollziehbar kontrolliert werden können.

Die Codes von Zahlenschlössern sollen regelmäßig geändert werden, insbesondere nach Beschaffung, beim Wechsel berechtigter Personen, nach Öffnungen in Abwe-

senheit von Nutzern oder bei Verdacht auf Kenntnisnahme durch Unbefugte, mindestens jedoch einmal jährlich. Dabei sind Codes so zu gestalten, dass sie keine leicht zu ermittelnden Zahlenfolgen enthalten.

Alle gültigen Codes sind nachvollziehbar zu dokumentieren und gesichert zu hinterlegen; eine Ablage im selben Schutzschrank ist unzulässig.

Sofern Schlüssel, Chips oder vergleichbare Identifikationsmittel eingesetzt werden, sind deren Verwaltung, Ausgabe, Hinterlegung, Sperrung und Rücknahme klar zu regeln. Bei Schutzschränken mit mehreren Sicherungsmechanismen, beispielsweise Kombinationen von Code und Schlüssel, ist festzulegen, ob die Hinterlegung gemeinsam oder getrennt erfolgt, wobei die Verfügbarkeit im Notfall und Sicherheitsanforderungen abzuwägen sind.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖNORM EN 1143-1	Wertbehältnisse – Anforderungen, Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Einbruchdiebstahl – Teil 1: Wertschutzschränke, Wertschutzschränke für Geldautomaten, Wertschutzraumtüren und Wertschutzräume

Stand: 01. Juni 2026

Tipps

Größe und Innenausstattung von Wertschutzschränken sollen dem vorgesehenen Verwendungszweck entsprechen und absehbare künftige Anforderungen berücksichtigen, da eine nachträgliche Anpassung nur eingeschränkt möglich ist und eine Unterdimensionierung typischerweise eine Neubeschaffung oder zusätzliche Aufstellung weiterer Schränke mit entsprechendem Aufwand nach sich zieht.

3 Elektronische Maßnahmen

Elektronische Maßnahmen umfassen alle sicherheitstechnischen Systeme zur Detektion und Überwachung sicherheitsrelevanter Ereignisse sowie zur Alarmierung und Steuerung von Sicherheits- und Interventionsmaßnahmen. Sie ermöglichen die frühzeitige Erkennung, Verifikation und Weiterleitung sicherheitsrelevanter Ereignisse und unterstützen eine koordinierte und zeitgerechte Reaktion.

Hierzu zählen insbesondere Einbruch- und Überfallmeldeanlagen einschließlich vorgeschalteter Perimeter-/Videoüberwachungssysteme, Zutrittskontrollsysteme sowie sicherheitstechnische Sensorik und zugehörige Steuerungs- und Übertragungseinrichtungen.

3.1 Einbruch- und Überfallmeldesysteme

Zur Sicherstellung einer zuverlässigen Detektion von Angriffsversuchen soll ein dem Risiko angemessenes Einbruch- und Überfallmeldesystem nach den Regeln der Technik umgesetzt werden.

Perimeter- und Freigeländeüberwachungssysteme ermöglichen eine vorgelagerte Detektion außerhalb der Gebäudehülle und sollen bei der Entwicklung des Schutzkonzepts risikobezogen geprüft und entsprechend dem Risiko berücksichtigt werden. Perimeter- und Freigeländeüberwachungssysteme sind in der Regel an die Einbruch- und Überfallmeldeanlage (EMA/ÜMA) gekoppelt und bilden so einen integralen Bestandteil des Gesamtsystems.

Sämtliche Sicherungsbereiche und Komponenten einer EMA/ÜMA sollen entsprechend dem entwickelten Schutzkonzept und passend zur zonalen Logik umgesetzt werden. Jene Gebäude, Räume und Öffnungselemente, die in den Überwachungsbereich einer EMA/ÜMA einbezogen werden, sollen sich in einem baulichen Zustand befinden, der den störungsfreien und bestimmungsgemäßen Betrieb der Anlage gewährleistet. Insbesondere sollen bauliche Mängel, die zu Falsch- oder Täuschungsalarmen führen können – etwa mangelhaft schließende Türen, Fenster oder Tore, verzogene Rahmen oder undichte Gebäudeöffnungen –, vor Inbetriebnahme der Anlage behoben werden.

Generell sollen Melder so installiert werden, dass die Erfassung von Angriffen maximiert und das Risiko von Falschalarmen minimiert wird.

Leitungswege für Alarmierung und Alarmübertragung sind so auszuführen, dass sie gegen Erkennung und gezielte Manipulation geschützt sind. Dies umfasst auch funkbasierte Übertragungsstrecken einschließlich Antennen und deren Anbindungsleitungen, die als Teil des Alarmübertragungswegs entsprechend zu schützen sind.

Insbesondere sind Leitungen möglichst verdeckt zu verlegen oder entsprechend baulich zu schützen. Übertragungswege sind nach Möglichkeit direkt und ohne erkennbare Führung in den gesicherten Bereich einzuführen und kritische Übergabepunkte in überwachten Bereichen anzuordnen. Ist eine ausreichend geschützte oder verdeckte Verlegung nicht möglich, sind geeignete alternative Maßnahmen vorzusehen, wie beispielsweise zusätzliche Übertragungswege oder redundante Kommunikationslösungen. Neben verifizierten sicherheitsrelevanten Ereignissen sollten auch technische Systemstörungen, Falsch- und Täuschungsalarme sowie sonstige Fehlalarme infolge von Bedien- oder Prozessfehlern, Umgebungseinflüssen oder anlagentechnischen Mängeln systematisch ausgewertet und geeignete Korrekturmaßnahmen abgeleitet werden, um die Systemintegrität dauerhaft aufrechtzuerhalten und einen wirksamen Betriebszustand der Anlagen auf lange Sicht zu gewährleisten.

Berechtigungssysteme zur Bedienung und Konfiguration der Anlage sind so auszulegen, dass die eingesetzten Identifikationsmittel eine dem Schutzbedarf entsprechende und ausreichend große Anzahl an Variationsmöglichkeiten aufweisen, um unbefugte Nutzung durch Erraten, Nachbildung oder Missbrauch wirksam zu verhindern.

Die festgelegten Anforderungen sind im Rahmen der Planung eindeutig zu dokumentieren, dauerhaft vorzuhalten und regelmäßig zu überprüfen sowie bei Änderungen fortzuschreiben. Dabei ist sicherzustellen, dass das System insgesamt konsistent und nachvollziehbar ausgelegt ist.

Die Dokumentation hat den gesamten Lebenszyklus des Systems zu unterstützen und insbesondere Grundlagen wie die spezifische Risikoanalyse, Anforderungen, Systemkonzept, Lage- und Ausführungsplanung sowie Prüf- und Inbetriebnahmekonzepte zu umfassen. Darüber hinaus sollen betriebsrelevante Unterlagen wie Bedien- und Schulungsunterlagen, Schnittstellenbeschreibungen sowie Wartungs- und Instandhaltungskonzepte vorgehalten werden.

Vor der Inbetriebnahme ist sicherzustellen, dass das System im Rahmen eines Probebetriebs unter realistischen Bedingungen getestet wird und die geforderten Funktionen, insbesondere Detektion, Alarmübertragung und Alarmverarbeitung, zuverlässig erfüllt. Eine endgültige Inbetriebnahme darf erst nach erfolgreicher Funktionsprüfung erfolgen. Der Betreiber sowie alle für die Bedienung verantwortlichen Personen sind angemessen zu schulen. Dabei ist insbesondere auf die korrekte Bedienung, die Vermeidung von Falschalarmen sowie die damit verbundenen organisatorischen Abläufe und Interventionsmaßnahmen hinzuweisen.

Der Betrieb des Systems ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen. Hierzu zählen insbesondere regelmäßige Funktionsprüfungen der Melder, Übertragungswege und Alarmierungseinrichtungen; präventive Wartungsmaßnahmen zur Sicherstellung der Funktionsfähigkeit sowie korrektive Maßnahmen zur Fehlerbehebung.

Regelmäßige Funktionsprüfungen (einschließlich abgestimmter Probealarme) sind durchzuführen und zu dokumentieren. Dabei ist sicherzustellen, dass die Alarmübertragung sowie die vorgesehenen Reaktionsprozesse ordnungsgemäß funktionieren. Sämtliche relevanten Betriebsereignisse, insbesondere Alarme, Störungen, Sabotagemeldungen, Prüfungen, Änderungen und Instandhaltungsmaßnahmen, sind nachvollziehbar zu protokollieren. Die gewonnenen Erkenntnisse sind systematisch auszuwerten und in eine kontinuierliche Verbesserung des Systems zu überführen.

Anforderungsmatrix

Die Anforderungen an Einbruch- und Überfallmeldeanlagen werden entsprechend der Kritikalität der betriebenen wesentlichen Dienste in drei Risikoklassen (Klasse A, Klasse B und Klasse C) unterteilt, wobei die Anforderungen mit steigender Klasse zunehmen. Die jeweils höhere Klasse umfasst dabei stets alle Anforderungen der niedrigeren Klasse/n und ergänzt diese um zusätzliche Anforderungen oder verschärft diese.

Diese Spezifikationen sind in einem eigenen Dokument geregelt, welches von der Behörde zur Verfügung gestellt wird.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
OVE EN 50131-1	Alarmanlagen – Einbruch- und Überfallmeldeanlagen – Teil 1: Systemanforderungen
ÖVE/ÖNORM EN 50131-2-x (Reihe)	Alarmanlagen – Einbruch- und Überfallmeldeanlagen – Teil 2-x
ÖVE/ÖNORM EN 50131-3	Alarmanlagen – Einbruch- und Überfallmeldeanlagen – Teil 3: Melderzentrale
OVE EN 50131-4	Alarmanlagen – Einbruch- und Überfallmeldeanlagen – Teil 4: Signalgeber
OVE EN 50131-5-3	Alarmanlagen – Einbruch- und Überfallmeldeanlagen – Teil 5-3: Anforderungen an Übertragungsgeräte, die Funkfrequenz-Techniken verwenden
OVE EN 50131-6	Alarmanlagen – Einbruch- und Überfallmeldeanlagen – Teil 6: Energieversorgungen
DIN CLC/TS 50131-7*VDE V 0830-2-7	Alarmanlagen – Einbruch- und Überfallmeldeanlagen – Teil 7: Anwendungsregeln
OVE EN 50131-8	Alarmanlagen – Einbruch- und Überfallmeldeanlagen – Teil 8: Nebelgeräte für Sicherungsanwendungen
DIN CLC/TS 50131-9*VDE V 0830-2-9	Alarmanlagen – Einbruch- und Überfallmeldeanlagen – Teil 9: Alarmvorprüfung – Verfahren und Grundsätze
ÖVE/ÖNORM EN 50131-10	Alarmanlagen – Einbruch- und Überfallmeldeanlagen – Teil 10: Anwendungsspezifische Anforderungen an Übertragungseinrichtungen
OVE TS 50131-12	Alarmanlagen – Einbruch- und Überfallmeldeanlagen – Teil 12: Methoden und Anforderungen zur Scharf- und Unscharfschaltung von Einbruchmeldeanlagen (EMA)
OVE EN 50136-1	Alarmanlagen – Alarmübertragungsanlagen und -einrichtungen – Teil 1: Allgemeine Anforderungen an Alarmübertragungsanlagen
OVE EN 50136-2	Alarmanlagen – Alarmübertragungsanlagen und -einrichtungen – Teil 2: Anforderungen an Übertragungseinrichtungen (ÜE)
OVE EN 50136-3	Alarmanlagen – Alarmübertragungsanlagen und -einrichtungen – Teil 3: Anforderungen an Übertragungszentralen (ÜZ)
DIN CLC/TS 50136-4*VDE V 0830-5-4	Alarmanlagen – Alarmübertragungsanlagen und -einrichtungen – Teil 4: Anzeige- und Bedieneinrichtung
DIN CLC/TS 50136-7*VDE V 0830-5-7	Alarmanlagen – Alarmübertragungsanlagen und -einrichtungen – Teil 7: Anwendungsregeln
DIN CLC/TS 50136-9*VDE V 0830-5-9	Alarmanlagen – Alarmübertragungsanlagen und -einrichtungen – Teil 9: Anforderungen an standardisierte Protokolle zur Alarmübertragung unter Nutzung des Internetprotokolls (IP)

Stand: 01. Juni 2026

Bezeichnung	*Spezifische Inhalte*
ÖVE/ÖNORM EN 50130-4	Alarmanlagen – Teil 4: Elektromagnetische Verträglichkeit – Produktfamiliennorm: Anforderungen an die Störfestigkeit von Anlageteilen für Brandmeldeanlagen, Einbruch- und Überfallmeldeanlagen, Video-Überwachungsanlagen, Zutrittskontrollanlagen sowie Personen-Hilferufanlagen
ÖVE/ÖNORM EN 50130-5	Alarmanlagen – Teil 5: Methoden für Umweltprüfungen
OVE-Richtlinie R 2 + A1	Einbruch- und Überfallmeldeanlagen – Planung, Einbau, Betrieb und Instandhaltung
VdS 3143	Sicherungsleitfaden Perimeter
DIN CLC/TS 50661-1*VDE V 0830-100-1	Alarmanlagen –Externe Perimeter-Sicherheitsanlagen – Teil 1: Systemanforderungen
DIN VDE V 0826-20*VDE V 0826-20	Überwachungsanlagen – Teil 20: Externe Perimeter-Sicherungsanlagen - Anwendungsregeln

Stand: 01. Juni 2026

Tipps

Da Detektionen im Außenbereich aufgrund von Umwelteinflüssen eine erhöhte Falschalarmrate aufweisen können, wird die Kombination mit Videoüberwachung zur Alarmverifikation empfohlen. Videoüberwachungssysteme können dabei gleichzeitig auch zur Detektion sicherheitsrelevanter Ereignisse im Freigelände eingesetzt werden. Bei der Auswahl geeigneter Technologien sind insbesondere die am jeweiligen Standort vorherrschenden Umweltbedingungen zu berücksichtigen.
Insbesondere die Detektion im Freien erfordert die Auswahl geeigneter Technologien in Hinblick auf die an der jeweiligen Liegenschaft vorherrschenden Umweltbedingungen (Tiere, Vegetation, Klima, Schattenwurf, Wind, Immissionen, Geländeaufbau etc.). Die genutzte Technologie ist entsprechend den Umweltbedingungen passend auszuwählen, um die gewünschte Detektion praktisch auch tatsächlich zu erwirken.
Falsch- bzw. Fehlalarme von Detektionssystemen, welche sich im Freibereich von Liegenschaften befinden, müssen infolge von Umwelteinwirkungen auch bei gut eingestellten Systemen nach den Regeln der Technik in gewissem Maß in Kauf genommen werden. Wenn Perimeter-Detektion aus der spezifischen Risikoanalyse als notwendige Maßnahme hervorgeht, müssen kritische Einrichtungen die für sie verhältsnimäßigen organisatorischen Maßnahmen umsetzen, sodass innerhalb und außerhalb regulärer Betriebszeiten Alarme angemessen verifiziert werden können und darauf reagiert werden kann. Dies umfasst auch die entsprechende Bereitstellung und Schulung von Personal oder die Auslagerung der Verifikation und Alarmierung an externe Dienstleister.

3.2 Videoüberwachungssysteme

Zur Sicherstellung einer dem Risiko angemessenen Überwachung und Dokumentation von Vorgängen in sicherheitsrelevanten Bereichen sind Videoüberwachungssysteme nach den Regeln der Technik zu planen, umzusetzen und zu betreiben.

Dies umfasst insbesondere die schwerpunktmäßige Überwachung von kritischen Infrastrukturen, deren Annäherungs- und Zugangspunkten sowie relevanten Bewegungs- und Fluchtwegen.

Auf Grundlage des Schutzkonzepts sind die allgemeinen Anforderungen an das System festzulegen, wobei eine differenzierte Betrachtung einzelner Systembereiche, Anwendungen und Funktionen erforderlich ist. Insbesondere sind sicherheitsrelevante Funktionen wie Kommunikationsverbindungen, Datenspeicherung und -archivierung, Protokollierung, Alarmverarbeitung, Systemüberwachung, Fehlererkennung, Energieversorgung, Zeitkonsistenz, Authentifizierung und Autorisierung, Datenkennzeichnung sowie der Schutz vor Manipulation gezielt und dem Risiko entsprechend abzusichern.

Des Weiteren hat die Planung von Videoüberwachungssystemen auf Basis klar definierter operativer Anforderungen zu erfolgen. Dabei ist insbesondere festzulegen, welche sicherheitsrelevanten Ereignisse oder Situationen erfasst werden sollen und unter welchen Rahmenbedingungen das System betrieben wird. Die Auslegung der einzelnen Überwachungsbereiche erfolgt szenariobasiert unter Berücksichtigung von Zielobjekten, Bewegungsmustern und Umgebungsbedingungen.

Für jeden Überwachungsbereich sind geeignete Anforderungen an Bildqualität und Auflösung festzulegen, sodass die angestrebte Erkennungsleistung zuverlässig erreicht wird. Maßgeblich hierfür ist insbesondere die im jeweiligen Überwachungsbereich tatsächlich erreichbare Bilddetailgenauigkeit am relevanten Objekt. Die erforderliche Pixeldichte ist im Rahmen der Kameraauslegung sicherzustellen. Anzeige- und Wiedergabesysteme dürfen diese Qualität nicht beeinträchtigen.

Die Anzahl, Positionierung und Ausrichtung der Kameras ist auf Basis der gewünschten Abdeckung und der erforderlichen Detailstufe festzulegen und zu dokumentieren. Dabei sind insbesondere Lichtverhältnisse, Blendung, Reflexionen, Witterungseinflüsse, Vegetation, saisonale Veränderungen sowie sonstige mögliche Sichtbehinderungen zu berücksichtigen. Beleuchtungseinrichtungen haben eine gleichmäßige Ausleuchtung von Eingängen, Parkplätzen, Gehwegen und Kamerasichtfeldern zu gewährleisten und dabei Blendung sowie starke Schattenbildung vermeiden, die die Erkennung oder Aufzeichnung beeinträchtigen könnten.

Die festgelegten Anforderungen sind im Rahmen der Planung eindeutig zu dokumentieren, dauerhaft vorzuhalten und regelmäßig zu überprüfen sowie bei Änderungen fortzuschreiben. Dabei ist sicherzustellen, dass das System insgesamt konsistent und nachvollziehbar ausgelegt ist. Der Betrieb des Systems ist durch geeignete sowie verhältnismäßige technische und organisatorische Maßnahmen

sicherzustellen. Für Abnahme und Betrieb sind geeignete Prüf- und Validierungskriterien (z.B. zu Bildqualität, Abdeckungsbereich und Erkennungsleistung) festzulegen, anhand derer die Funktionsfähigkeit nachweisbar überprüft werden kann.

Not- und Ersatzbeleuchtung sollte regelmäßig getestet werden. Abhilfemaßnahmen (z.B. Austausch von Leuchtmitteln, Anpassung der Abdeckung, Rückschnitt von Vegetation) sind regelmäßig durchzuführen. Die Zeitsynchronisation der Überwachung, der Aufzeichnungsstatus sowie die Aufbewahrungsfristen sind regelmäßig zu überprüfen. Einrichtungen haben routinemäßige Wiedergabeprüfungen durchzuführen, um zu überprüfen, dass Gesichter, Handlungen und Ereignisse für die vorgesehenen forensischen Zwecke nach potenziellen Vorfällen identifizierbar sind.

Ein Ersatz für kritische Komponenten (z.B. Speichermedien, Energieversorgungseinheiten) sollte in entsprechendem Umfang vorgehalten werden. Erkenntnisse aus Betrieb, Störungen und Prüfungen sollen systematisch ausgewertet und zur kontinuierlichen Verbesserung des Systems herangezogen werden.

Die Dokumentation soll den gesamten Lebenszyklus des Systems unterstützen und insbesondere Grundlagen wie die spezifische Risikoanalyse, Anforderungen, Systemkonzept, Lage- und Ausführungsplanung, Prüf- und Inbetriebnahmekonzepte sowie Grundlagen und Ergebnisse der Tests und Abnahmen umfassen. Darüber hinaus sind betriebsrelevante Unterlagen wie Bedien- und Schulungsunterlagen, Schnittstellenbeschreibungen sowie Wartungs- und Instandhaltungskonzepte vorzuhalten.

Anforderungsmatrix

Die Anforderungen an Videoüberwachungssysteme werden entsprechend der Kritikalität des betriebenen wesentlichen Dienstes in drei Risikoklassen unterteilt – Klasse A, Klasse B und Klasse C –, wobei die Anforderungen mit steigender Klasse zunehmen. Die jeweils höhere Klasse umfasst dabei stets alle Anforderungen der niedrigeren Klasse/n und ergänzt diese um zusätzliche Anforderungen oder verschärft diese.

Diese Spezifikationen sind in einem eigenen Dokument geregelt, welches von der Behörde zur Verfügung gestellt wird.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖVE/ÖNORM EN 62676-1-1	Videoüberwachungsanlagen für Sicherheitsanwendungen – Teil 1-1: Systemanforderungen – Allgemeines
ÖVE/ÖNORM EN 62676-1-2	Videoüberwachungsanlagen für Sicherungsanwendungen – Teil 1-2: Allgemeine Anforderungen an die Videoübertragung
ÖVE/ÖNORM EN 62676-2-1	Videoüberwachungsanlagen für Sicherungsanwendungen – Teil 2-1: Videoübertragungsprotokolle - Allgemeine Anforderungen

Stand: 01. Juni 2026

Bezeichnung	*Spezifische Inhalte*
ÖVE/ÖNORM EN 62676-2-2	Videoüberwachungsanlagen für Sicherungsanwendungen – Teil 2-2: Videoübertragungsprotokolle - IP-Interoperabilität auf Basis von HTTP- und REST-Diensten
ÖVE/ÖNORM EN 62676-3	Videoüberwachungsanlagen für Sicherungsanwendungen – Teil 3: Analoge und digitale Videoschnittstellen
OVE EN 62676-4	Videoüberwachungsanlagen für Sicherungsanwendungen – Teil 4: Anwendungsregeln
OVE-Richtlinie R 9	Alarmanlagen – CCTV-Überwachungsanlagen für Sicherungs-anwendungen – Planung, Einbau, Betrieb und Instandhaltung

Stand: 01. Juni 2026

Tipps

Videoüberwachungssysteme übernehmen eine wesentliche Rolle bei der Verifikation von Alarmen und ermöglichen eine lagebezogene Bewertung von Ereignissen. Dadurch kann das Schutzkonzept im Betrieb wirksam umgesetzt und unterstützt werden. Darüber hinaus können Videoüberwachungssysteme – beispielsweise durch bewegungs- oder ereignisbasierte Auswerteverfahren – auch zur Detektion von sicherheitsrelevanten Vorgängen eingesetzt werden.

3.3 Zutrittskontrollsysteme

Zur Sicherstellung einer dem Risiko angemessenen Zutrittssteuerung soll ein elektronisches Zutrittskontrollsystem nach den Regeln der Technik umgesetzt werden.

Zutrittskontrollsysteme sollen die Authentizität von Zutrittsvorgängen gewährleisten, sodass die Identität der zutretenden Person sowie der Zeitpunkt und Ort des Zutritts nachvollziehbar und nicht abstreitbar dokumentiert werden (Non-Repudiation). Die Zuordnung von Handlungen zu Personen soll durchgängig sichergestellt sein (Accountability). Die dabei erzeugten Protokolldaten sollen dem jeweiligen Risiko entsprechend angemessen geschützt gespeichert werden.

Ein technischer Sicherungsbereich kann in mehrere Raumzonen unterteilt werden. Raumzonen müssen entsprechend der zonalen Struktur immer geschlossene Einheiten bilden und eine kongruente Schutzfunktion bieten.

Zutrittskontrollanlagen sollen stets in einen geeigneten organisatorischen Rahmen eingebettet sein. Dies soll insbesondere auch die Auswertung von Protokollen und den Umgang mit Auffälligkeiten umfassen, da die Schutzwirkung der Anlage wesentlich vom Zusammenwirken technischer und organisatorischer Maßnahmen abhängt.

Die auf Zutritt zu überwachenden Objekte sollen sich in einem baulichen Zustand befinden, der den störungsfreien und bestimmungsgemäßen Betrieb der Zutrittskontrollanlage gewährleistet. Insbesondere sollen mangelhaft schließende Sperren wegen der sonst bestehenden Gefahr von Täuschungsalarmen unverzüglich instand gesetzt werden.

Alle sicherheitsrelevanten Anlagenteile der Zutrittskontrollanlage sollen sabotageüberwacht ausgeführt und so eingebunden sein, dass unbefugte Eingriffe oder Gehäuseöffnungen zuverlässig erkannt und alarmiert werden.

Leitungen der Zutrittskontrollanlage sollen grundsätzlich innerhalb von Sicherungsbereichen betriebssicher und möglichst unauffällig verlegt werden (z.B. unter Putz). Außerhalb von Sicherungsbereichen verlegte Leitungen sollen nicht als Bestandteil der Zutrittskontrollanlage erkennbar sein.

Bei vernetzten bzw. online angebundenen Zutrittskontrollanlagen sollen sicherheitsrelevante Ereignisse, Störungen und Sabotagezustände an den zuständigen Zentralen oder Anzeige- und Bedieneinrichtungen in eindeutig zuordenbarer Form angezeigt werden. Es soll sichergestellt werden, dass eine festgelegte Stelle diese Meldungen entgegennimmt, bewertet und innerhalb der vorgegebenen Reaktionszeiten nach festgelegten Verfahren bearbeitet. Bei nicht vernetzten bzw. Offline-Zutrittskontrollanlagen sind diese Themen organisatorisch bestmöglich zu kompensieren.

Bei kombinierten Systemen sind alle Funktionen, die zum bestimmungsgemäßen Betrieb des Gesamtsystems erforderlich sind, auf die Systeme ZKA und EMA verteilt. Zusätzliche Funktionen, die auch Teil anderer Systeme sein können, sind zulässig, wenn diese – auch bei Störungen – die Funktionen der Einzelsysteme nicht negativ beeinflussen.

Funktionen und Bedienungen der Teilsysteme dürfen nicht zu sicherheitsgefährdenden und sicherheitsmindernden Auswirkungen im Teilsystem EMA führen (rückwirkungsfreie Ausführung).

Bei ZKA-Anlagenteilen, die über ZKA/EMA-Schnittstelle Funktionen einer EMA übernehmen, gelten dieselben Anforderungen für die Überbrückungszeit der Notstromversorgung wie für die EMA.

Die festgelegten Anforderungen sind im Rahmen der Planung eindeutig zu dokumentieren, dauerhaft vorzuhalten, regelmäßig zu überprüfen und bei Änderungen fortzuschreiben. Dabei ist sicherzustellen, dass das System insgesamt konsistent, nachvollziehbar und entsprechend dem Schutzbedarf der jeweiligen Zutrittspunkte ausgelegt ist.

Die Dokumentation soll den gesamten Lebenszyklus der Zutrittskontrollanlage unterstützen und insbesondere Grundlagen wie die spezifische Risikoanalyse, Anforderungen, Systemkonzept, Zonen- und Berechtigungskonzept, Lage- und

Ausführungsplanung, Türlisten, Schnittstellen, Prüf- und Inbetriebnahmekonzepte sowie die Ergebnisse von Tests, Abnahmen, Änderungen und Instandhaltungsmaßnahmen umfassen. Darüber hinaus sollen betriebsrelevante Unterlagen wie Bedien- und Schulungsunterlagen, Wartungs- und Instandhaltungsvorgaben, Ereignis- und Betriebsdokumentationen sowie Unterlagen zu Erweiterungen und Anpassungen vorgehalten werden.

Vor der Übergabe ist sicherzustellen, dass die errichtete Anlage mit der freigegebenen Planung bzw. Bestandsdokumentation übereinstimmt und die für Betrieb, Bedienung, Störungsbehandlung und Instandhaltung erforderlichen Unterlagen vollständig übergeben werden. Die übergebenen Unterlagen sind vom Betreiber der kritischen Einrichtung sicher aufzubewahren.

Der Betrieb der Zutrittskontrollanlage ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen. Hierzu zählen insbesondere eine ordnungsgemäße Bedienung entsprechend den Herstellervorgaben, regelmäßige Funktionsprüfungen, präventive Wartungsmaßnahmen, die unverzügliche Behandlung von Störungen und Unregelmäßigkeiten sowie die sichere Fortschreibung von System-, Konfigurations- und Berechtigungsdaten.

Für die eingesetzten Identifikationsmittel sollen geeignete Verfahren zur Überwachung der Gebrauchstauglichkeit und zum rechtzeitigen Austausch festgelegt werden, um eine zuverlässige Funktion dauerhaft sicherzustellen. Vor der Inbetriebnahme bzw. Übergabe soll sichergestellt werden, dass die Anlage im Rahmen von Sicht-, Funktions- und gegebenenfalls Probebetrieb unter realistischen Bedingungen geprüft wurde und die vorgesehenen Funktionen, Anzeigen, Schnittstellen und gegebenenfalls Notstromfunktionen ordnungsgemäß arbeiten. Der Betreiber sowie die für Bedienung und Verwaltung verantwortlichen Personen sind angemessen einzuweisen.

Alle relevanten Betriebsereignisse, insbesondere Freigabe-, Störungs-, Sabotage- und sonstige sicherheitsrelevante Meldungen, Prüfungen, Änderungen, Erweiterungen und Instandhaltungsmaßnahmen, sind nachvollziehbar zu dokumentieren. Erkenntnisse aus Betrieb, Meldungen, Störungen, Prüfungen und Instandhaltungsmaßnahmen sind systematisch auszuwerten und für eine kontinuierliche Verbesserung des Systems zu nutzen.

Für sicherheitsrelevante Meldungen soll sichergestellt werden, dass diese an einer festgelegten Stelle auflaufen, dort bewertet und innerhalb der vorgegebenen Reaktionszeiten bearbeitet werden können. Soweit erforderlich, sollen hierfür auch Vertretungs- und Weiterleitungsregelungen bestehen.

Für den Fall eines teilweisen oder vollständigen Ausfalls der Zutrittskontrollanlage sind organisatorische Ersatzmaßnahmen festzulegen, um die Zutrittsregelung und den Schutz sicherheitsrelevanter Bereiche weiterhin angemessen aufrechterhalten zu können. Änderungen, Ergänzungen und Erweiterungen an der Zutrittskontroll-

anlage sollen nur durch fachkundige und hierzu geeignete Stellen durchgeführt, in Bezug auf ihre Auswirkungen auf das Gesamtsystem bewertet und in die fortgeschriebene Dokumentation übernommen werden.

Anforderungsmatrix

Die Anforderungen an Zutrittskontrollanlagen werden entsprechend der Kritikalität des betriebenen wesentlichen Dienstes in drei Risikoklassen (Klasse A, Klasse B und Klasse C) unterteilt, wobei die Anforderungen mit steigender Klasse zunehmen. Die jeweils höhere Klasse umfasst dabei stets alle Anforderungen der niedrigeren Klasse/n und ergänzt diese um zusätzliche Anforderungen oder verschärft diese.

Diese Spezifikationen sind in einem eigenen Dokument geregelt, welches von der Behörde zur Verfügung gestellt wird.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖVE/ÖNORM EN 60839-11-1	Alarmanlagen – Teil 11-1: Elektronische Zutrittskontrollanlagen – Anforderungen an Anlagen und Geräte
ÖVE/ÖNORM EN 60839-11-2	Alarmanlagen – Teil 11-2: Elektronische Zutrittskontrollanlagen –- Anwendungsregeln
OVE EN IEC 60839-11-5	Alarmanlagen – Teil 11-5: Elektronische Zutrittskontrollanlagen – Open Supervised Device Protocol (OSDP)
DIN EN 60839-11-31*VDE 0830-81-11-31	Alarmanlagen – Teil 11-31: Elektronische Zutrittskontrollanlagen – Basis Kommunikationsprotokoll basierend auf Web Services
OVE EN 60839-11-32	Alarmanlagen – Teil 11-32: Elektronische Zutrittskontrollanlagen – Überwachung der Zutrittskontrolle basierend auf Web Services
OVE EN IEC 60839-11-33	Alarmanlagen – Teil 11-33: Elektronische Zutrittskontrollanlagen – Parametrierung der Zutrittskontrolle basierend auf Web Services
OVE-Richtlinie R 10	Alarmanlagen – Zutrittskontrollanlagen – Planung, Einbau, Betrieb und Instandhaltung

Stand: 01. Juni 2026

Tipps

Die Nutzung webbasierter Schnittstellen gemäß EN 60839-11-31 ff. ist bei entsprechend sicherer Systemarchitektur zulässig, sofern sicherheitskritische Funktionen lokal verbleiben und externe Schnittstellen angemessen abgesichert sind. Webbasierte Bedienoberflächen sind dabei nicht mit cloudbasierten Systemen gleichzusetzen; die Wahl des Protokolls und die Gestaltung des

Frontends obliegen der herstellerspezifischen Umsetzung, wobei den Regeln der Technik entsprechende Sicherheitsstandards einzuhalten sind.
Sowohl cloudbasierte als auch lokal oder im Kundennetzwerk gehostete Systeme sollen den Regeln der Technik entsprechend umgesetzt werden, insbesondere im Hinblick auf Cybersicherheit, Resilienz und Verschlüsselung. Bei der Beschaffung soll darauf geachtet werden, dass die eingesetzten Systeme und Komponenten den Anforderungen der einschlägigen EU-Rechtsakte entsprechen, insbesondere jenen der Cyberresilienz-Verordnung (EU) 2024/2847 (Cyber Resilience Act – CRA).
Elemente zur Auslösung einer Notsperre (z.B. bei Bedrohungslagen, Notfällen oder sicherheitsrelevanten Vorfällen) sollen mindestens den Sicherheitsanforderungen der vorhandenen Zutrittskontrollanlage entsprechen, damit sie nicht als Angriffspunkt zur Umgehung der regulären Zutrittssteuerung genutzt werden können.
Bei Online-Zutrittskontrollanlagen soll jede Betätigung einer Notsperre eine Meldung an die Zutrittskontrollzentrale auslösen und protokolliert werden. Die Meldung soll an einer festgelegten Stelle bewertet und innerhalb der vorgegebenen Reaktionszeiten nach festgelegten Verfahren bearbeitet werden.
Notausgänge und Fluchtwege sollen in Fluchtrichtung jederzeit frei passierbar sein und gleichzeitig alarmtechnisch überwacht werden. Bei vernetzten Zutrittskontrollanlagen kann dies über die Türzustandsüberwachung der Zutrittskontrollanlage oder über die Einbruchmeldeanlage erfolgen. Verfügen Notausgänge über keine Türzustandsüberwachung, soll die Öffnung durch geeignete Detektionseinrichtungen (z.B. Druckstangenmelder, Riegelkontakte) erfasst werden. Jede Öffnung eines alarmgesicherten Notausgangs soll eine Meldung auslösen, die an einer festgelegten Stelle bewertet und erst nach bewusster Rücksetzung in den Normalzustand überführt wird.

4 Organisatorische und personelle Maßnahmen

Organisatorische und personelle Maßnahmen ergänzen bauliche und technische Vorkehrungen und bilden gemeinsam mit diesen ein wirksames Schutzkonzept. Organisatorische Maßnahmen regeln die Steuerung, Dokumentation und Überwachung sicherheitsrelevanter Abläufe. Personelle Maßnahmen betreffen Auswahl, Qualifikation, Schulung und Einsatz der mit Sicherheitsaufgaben betrauten Personen.

Die nachfolgenden Anforderungen zur Zutritts- und Zugriffssteuerung sowie zum Schutz sensibler Informationen gelten unbeschadet der Verpflichtungen zum Cybersicherheits-Risikomanagement nach der NIS-2-Richtlinie und den einschlägigen Vorgaben. Bestehende Maßnahmen aus diesem Bereich sollten, soweit möglich, integriert und nicht parallel aufgebaut werden.

4.1 Steuerung von Zutritt und physischem Zugriff

Relevante Bereiche sollen eine zonale Sicherheitsstruktur aufweisen, die durch eine Kombination aus technischen, organisatorischen und personellen Maßnahmen

entsprechend dem Schutzkonzept gesteuert wird und den Zutritt zu Zonen sowie den physischen Zugriff auf die darin befindlichen Schutzgüter für definierte Personengruppen angemessen beschränkt.

Die übergeordnete Zoneneinteilung kann beispielhaft eine Differenzierung in öffentliche, Arbeits-, eingeschränkte und kritische Zonen umfassen und sich am Schutzbedarf der jeweiligen Schutzgüter in den Bereichen orientieren.

Generell ist der Zugang von Fahrzeugen, Personal und Gütern zu relevanten Räumlichkeiten über eine begrenzte Anzahl kontrollierbarer Kontrollpunkte zu führen. Die Zonen sollen insbesondere jene Bereiche umfassen, die für die Erbringung des wesentlichen Dienstes relevant sind oder einen erhöhten Schutzbedarf aufweisen. Dazu zählen beispielsweise Technikräume, Verteilerinfrastruktur sowie physisch gesicherte Leitungs- und Trassenführungen. Die Zonen sollen bei Bedarf weiter granular spezifiziert werden.

In geregelten Zonen sollen einheitliche Sicherheitsregeln (z.B. Kennzeichnungs- und Ausweispflicht, Meldepflichten, Bestimmungen für das Mitführen von Geräten) gelten.

Die personelle Steuerung der Zutritts- und Zugriffsberechtigungen, insbesondere die rollenbasierte Vergabe, die Anwendung des Prinzips der geringsten Privilegien/ des Prinzips der minimalen Rechtevergabe, die anlassbezogene Überprüfung bei Rollenwechsel oder Ausscheiden sowie die Verantwortlichkeiten für die Berechtigungssteuerung, wird im Leitfaden Z 5 geregelt.

Zutritte zu Zonen sowie physische Zugriffe auf Anlagen, Objekte und Schutzgüter sollen dem Risiko entsprechend protokolliert werden und eine entsprechende Beweissicherung berücksichtigt werden. Die Protokolldaten sind dem jeweiligen Risiko entsprechend geschützt zu speichern. Für alle relevanten Anlagen, Objekte, Zonen und Schutzgüter soll festgelegt sein, welche Maßnahmen bei versuchtem unerlaubtem Zutritt oder Zugriff zu ergreifen sind. Unabhängig davon soll festgelegt werden, wie in Ausnahmesituationen (Evakuierung etc.) zu verfahren ist.

Sofern ein Portierdienst, ein Empfang oder eine vergleichbare Stelle eingesetzt ist, soll diese den Personen- und, soweit erforderlich, den Fahrzeugverkehr an Gebäudezugängen, Zufahrten und sicherheitsrelevanten Bereichen im Rahmen der festgelegten Regelungen kontrollieren und überwachen sowie in die Besucherabwicklung einschließlich Registrierung und Ausgabe von Besucher- und temporären Zufahrtsausweisen eingebunden sein. Aufgaben, Zuständigkeiten und Schnittstellen sollen dokumentiert und bei mehreren Kontrollstellen so abgestimmt sein, dass eine lückenlose Kontrolle sichergestellt ist.

Informationen über Lage, Schutzmaßnahmen, Belegung, Abläufe und sicherheitsrelevante Tätigkeiten in geregelten Zonen und Sicherheitsbereichen sollen nach dem Need-to-know-Prinzip behandelt und nur an berechtigte Personen weitergegeben werden.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖVE/ÖNORM EN ISO/IEC 27002	Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Informationssicherheitsmaßnahmen
ÖISHB	Österreichisches Informationssicherheitshandbuch
NIS Fact Sheet 9/2022	Sicherheitsmaßnahmen für Betreiber wesentlicher Dienste

Stand: 01. Juni 2026

4.2 Verwaltung von Schlüsseln, Zutrittskontrollmedien und Identifikationsmitteln

Für alle relevanten Anlagen, Objekte und Zonen soll ein aktuelles, zentrales und maßgebliches Schließ- und Berechtigungsverzeichnis geführt werden, das die Zuordnung von Schlüsseln, Zutrittskontrollmedien und Identifikationsmitteln zu Bereichen, Schließgruppen und berechtigten Personen nachvollziehbar abbildet.

Die Herstellung, Ausgabe, Verwaltung, Aufbewahrung, Rückgabe und der Entzug dieser Mittel sollen zentral geregelt und nachvollziehbar dokumentiert sein. Die Ausgabe soll gegen Bestätigung erfolgen.

Schließ- bzw. bereichsbezogene Berechtigungsgruppen sollen so festgelegt sein, dass Zutritte entsprechend dem Schutzbedarf und den funktionalen Erfordernissen differenziert gesteuert werden können. Bei Bedarf sollen einzelne Räumlichkeiten, Bereiche oder Schutzgüter hiervon ausgenommen und separat gesichert werden können.

Für den Verlust, die Duplizierung, den Missbrauch oder den Verdacht einer Kompromittierung von Schlüsseln, Zutrittskontrollmedien und Identifikationsmitteln sowie bei Wegfall der Berechtigung sind verbindliche Maßnahmen festzulegen.

Diese sollen insbesondere Meldepflichten, die unverzügliche Sperrung, Entziehung oder Einziehung der betroffenen Mittel sowie erforderliche Ersatz- und Kostenregelungen umfassen.

Sofern ein Kompromittierungsverdacht besteht oder dies aufgrund der einrichtungsinternen Risikoanalyse erforderlich ist, sollen betroffene Schließungen, Schließzylinder oder Schließanlagen neu kodiert, ausgetauscht oder ersetzt werden.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖVE/ÖNORM EN ISO/IEC 27002	Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Informationssicherheitsmaßnahmen
ÖISHB	Österreichisches Informationssicherheitshandbuch
NIS Fact Sheet 9/2022	Sicherheitsmaßnahmen für Betreiber wesentlicher Dienste

Stand: 01. Juni 2026

4.3 Poststellen und Lieferdepots

Poststellen, Lieferdepots sowie Warenannahme-, Anlieferungs- und Ladebereiche sollten vom sonstigen Betrieb räumlich getrennt angeordnet sein, den Warenfluss entsprechend der Vorgaben steuern und in der Lage sein, potenziell verdächtige Sendungen zu separieren und sicher zu überprüfen.

Aufgrund des regelmäßigen Personen- und Warenverkehrs erfordern diese Bereiche besondere Aufmerksamkeit hinsichtlich der Zutrittskontrolle. Sie sollten so gestaltet und betrieben werden, dass unbefugte Personen nicht über sie auf das Gelände oder in Gebäude gelangen und Lieferpersonal beim Be- und Entladen keinen Zugang zu weiterführenden Gebäudebereichen erhält. Übergänge zu angrenzenden geregelten oder kritischen Zonen sollten entsprechend gesichert sein, um eine Ausnutzung der Anlieferungsvorgänge zum unbefugten Eindringen zu verhindern.

Das Personal sollte über klare Verfahren im Umgang mit verdächtigen Sendungen informiert sein, einschließlich Maßnahmen zur Isolation, Deeskalation und Meldung an relevante interne und externe Stellen.

Öffnungswerkzeuge und persönliche Schutzausrüstung haben, sofern verhältnismäßig, zur Verfügung zu stehen.

Die Verwahrungskette (Chain of Custody) für wertvolle oder kontrollierte Lieferungen ist nachvollziehbar zu dokumentieren.

4.4 Schutz sensibler Informationswerte

Für sensible Informationswerte soll ein Verzeichnis und/oder ein Verwahrungsort eingerichtet und aufrechterhalten werden. Informationswerte sollten entsprechend dem Grad ihrer geschäftlichen oder sicherheitsbezogenen Sensibilität klassifiziert werden. In der Folge sollten kritische Einrichtungen ein Schema zur Dokumentation von Informationswerten (z.B. eingeschränkt, intern, öffentlich) anwenden und diese entsprechend kennzeichnen und handhaben. Zugriffe sind zu protokollieren. Die Regeln und Verfahren zur Klassifizierung und Handhabung sollten allen relevanten Mitarbeitenden kommuniziert und regelmäßig überprüft werden. Dies umfasst auch Regelungen zum Zugriff auf Informationen am Arbeitsplatz und Bildschirm sowie zur Erstellung oder Vervielfältigung von Informationen.
Soweit angemessen, haben kritische Einrichtungen die nationalen Vorschriften zum

Schutz klassifizierter Informationen, die als für die nationale Sicherheit relevant eingestuft sind, anzuwenden.

Wenn externe Akteure Zugriff auf Informationswerte benötigen, sollten kritische Einrichtungen Benutzerrichtlinien und Vertraulichkeitsvereinbarungen (Non-Disclosure Agreements) oder andere geeignete vertragliche Regelungen erstellen.

Alle kritischen Infrastrukturen, in denen sensible Informationswerte untergebracht sind (z B. Archive, Serverräume etc.), sowie andere Bereiche, aus denen sensible Informationswerte potenziell entnommen werden könnten, sind als Sicherheitszonen auszuweisen und mit besonders strengen Zutritts-, Einsichts- und Entnahmekontrollen zu überwachen.

Zugriffsrechte sollten regelmäßig geprüft und überprüft werden. Für sensible Informationswerte sollten Aufbewahrungsfristen festgelegt werden. Sobald diese Fristen überschritten wurden oder andere Entwicklungen eine Neuklassifizierung von Informationswerten erforderlich machen, sind geeignete Maßnahmen zu ergreifen, um Informationen zu bereinigen oder zu vernichten.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖVE/ÖNORM EN ISO/IEC 27002	Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Informationssicherheitsmaßnahmen
ÖISHB	Österreichisches Informationssicherheitshandbuch
NIS Fact Sheet 9/2022	Sicherheitsmaßnahmen für Betreiber wesentlicher Dienste

Stand: 01. Juni 2026

4.5 Personelle Maßnahmen

Kritische Einrichtungen sollen in Betracht ziehen, ausreichend Sicherheitspersonal vor Ort vorzuhalten, das mit der Durchführung von Streifengängen, Präsenzbewachung sowie der Steuerung der Zutrittskontrolle zu relevanten Einrichtungen, Zugängen oder Ausrüstungen betraut ist.

Das Sicherheitspersonal soll einen engen und regelmäßigen Kontakt zu den zuständigen Behörden aufrechterhalten. Das eingesetzte Personal soll entsprechend dem Risiko ausgewählt, zuverlässigkeitsüberprüft und geschult werden.

Alarme sollen entsprechend dem Risiko an eine personell besetzte Alarmempfangsstelle weitergeleitet werden, um eine Verifikation durch geschultes Personal zu ermöglichen. Ebenso soll die Funktionsfähigkeit der eingesetzten elektronischen Alarmierungs-, Überwachungs- und Kontrollsysteme personell überwacht werden und Alarmempfangsstellen sollen nach den Regeln der Technik betrieben werden.
Je nach organisatorischen Gegebenheiten ist eine geeignete Lösung zu wählen.

Alarme sollen stets an eine nach den Regeln der Technik betriebene Alarmempfangsstelle weitergeleitet werden. Kritische Einrichtungen ohne eigene besetzte Sicherheitsleitstelle sollen eine externe Alarmempfangsstelle beauftragen. Ist die eigene Sicherheitsleitstelle nur teilweise besetzt, soll außerhalb der Besetzungszeiten ein Dienstleister beauftragt werden. Bei einer ständig besetzten Sicherheitsleitstelle kann die Alarmempfangsstelle in den Leitstand integriert werden.

Im Alarmfall soll die Verständigung der zuständigen Interventionskräfte unverzüglich erfolgen. Art und Umfang der Intervention sollen dem jeweiligen Risiko und der zu erwartenden Täterqualität angemessen sein. Die Intervention kann durch die örtlich zuständige Exekutive, durch externe Interventionsdienste, durch internes Sicherheitspersonal oder durch Kombinationen dieser Varianten durchgeführt werden. Interventionskräfte sollen mit den anlagenspezifischen Gegebenheiten und Gefahren vertraut, entsprechend geschult und eingewiesen sein.

Bestreifungen sollen in risikobasierten, regelmäßigen, jedoch zeitlich unvorhersehbaren Intervallen erfolgen.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖNORM EN 17483-1	Private Sicherheitsdienstleistungen – Schutz kritischer Infrastrukturen –– Teil 1: Allgemeine Anforderungen
ÖNORM EN 17483-2	Private Sicherheitsdienstleistungen – Schutz kritischer Infrastrukturen – Teil 2: Flughafen- und Luftsicherheitsdienstleistungen
ÖNORM EN 17483-3	Private Sicherheitsdienstleistungen – Schutz kritischer Infrastrukturen – Teil 3: Sicherheitsdienstleistungen für Seeschifffahrt und Seehäfen
ÖNORM EN 17483-4	Private Sicherheitsdienstleistungen – Schutz kritischer Infrastrukturen – Teil 4: Sicherheitsdienstleistungen im Energiesektor
OVE EN 50518	Alarmempfangsstelle
NIS Fact Sheet 9/2022	Sicherheitsmaßnahmen für Betreiber wesentlicher Dienste

Stand: 01. Juni 2026

5 Maßnahmen im Umgang mit Bedrohungen durch unbemannte Systeme

Im Hinblick auf die von unbemannten Systemen ausgehenden Bedrohungen sollen kritische Einrichtungen Maßnahmen umzusetzen, die die Erkennung, Verfolgung und Identifizierung unbemannter Systeme ermöglichen (z.B. durch Radarsysteme, Funkfrequenzscanner, Tageslicht-/Wärmebildkameras, akustische Sensoren).

Um Spionage oder Überwachung durch nicht-kooperative unbemannte Systeme zu minimieren, sollen kritische Einrichtungen die Sichtbarkeit kritischer Infrastrukturen (aus der Luft, vom Wasser oder vom Boden aus) z.B. durch Verdeckung oder Umpositionierung reduzieren oder diese – soweit angemessen – in geschlossenen Räumlichkeiten unterbringen.

Die Bedrohung von Sabotage durch nicht-kooperative unbemannte Systeme gegen kritische Infrastrukturen ist ebenfalls zu reduzieren, z.B. durch Netze oder Überdachungen zur Drohnenabwehr, explosionshemmende Fenster, die Verstärkung von Dachstrukturen oder vollständige bauliche Einhausungen.

Mit der Weiterentwicklung technischer Fähigkeiten und sofern durch den regulatorischen Rahmen unterstützt, können kritische Einrichtungen auch die schrittweise Nutzung von Geofencing-Funktionalitäten in Betracht ziehen. Geofencing kann als präventive Schutzmaßnahme dienen, indem die Wahrscheinlichkeit unbeabsichtigter Eindringversuche regelkonformer Drohnen in sensible Bereiche reduziert wird.

Insbesondere im Bereich der Abwehr von unbemannten Systemen sollen kritische Einrichtungen die Zusammenarbeit mit Behörden und Akteuren suchen, die rechtlich zur Neutralisierung befugt sind (z.B. durch Funkfrequenzstörung, Überlagerungssignale oder andere kinetische oder nicht-kinetische Maßnahmen).

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
CWA 18150	Unmanned aircraft systems – Counter UAS – Testing methodology
EASA DIMA	Drone Incident Management at Aerodromes

Stand: 01. Juni 2026

6 Gesamtkonzept

Erst die Gesamtbetrachtung in einem Schutzkonzept Physischer Schutz erlaubt eine belastbare Beurteilung der Angemessenheit und Wirksamkeit. Einzelne Räumlichkeiten, Zonen oder Einzelmaßnahmen können isoliert weder hinsichtlich ihrer Schutzwirkung noch hinsichtlich ihrer Verhältnismäßigkeit bewertet werden, da sich die tatsächliche Resilienz erst aus dem Zusammenspiel von Detektion, Widerstandszeit, Alarmierung und Intervention ergibt. Ein für sich betrachtet „schwacher" Bereich kann im Gesamtgefüge durch vorgelagerte oder kompensierende Maßnahmen ausreichend geschützt sein. Umgekehrt kann eine vermeintlich hochwertige Einzelmaßnahme im Gesamtzusammenhang ihre Wirkung verfehlen, wenn sie nicht in das Schutzkonzept eingebettet ist.

Um in Österreich über die verschiedenen Sektoren und wesentlichen Dienste hinweg ein einheitliches Schutzniveau zu erreichen und den kritischen Einrichtungen zugleich eine praxistaugliche Orientierung zu bieten, gibt es, wie bereits dargestellt, eine Einteilung in drei Risikoklassen entsprechend der Kritikalität des betriebenen wesentlichen Dienstes. Diese fachlich fundierte und systematisch abgeleitete Einstufung der wesentlichen Dienste gemäß Delegierter Verordnung (EU) 2023/2450 in die drei Risikoklassen – Klasse A, Klasse B und Klasse C – erfolgte auf Basis der Regeln der Technik, der für die wesentlichen Dienste relevanten Ergebnisse der nationalen Risikoanalyse sowie auf einer Einschätzung von Expertinnen und Experten.
In einem weiteren Schritt wurden für diese drei Risikoklassen spezifische Vorgaben, insbesondere in Bezug auf Einbruch- und Überfallmeldesysteme, Videoüberwachungs- und Zutrittssteuerungssysteme, festgelegt. Auf diese Weise ergibt sich ein Referenzniveau für kritische Einrichtungen, das als Ausgangspunkt für die konkrete Ausgestaltung der Resilienzmaßnahmen herangezogen werden kann.

Das Ausmaß und der Umfang der tatsächlichen Umsetzung bleiben dabei stets Ergebnis der einrichtungsspezifischen Bedrohungs- und Risikoanalyse sowie spezifischer Risikobewertungen; es wird jedoch davon ausgegangen, dass zumindest ein Bereich bei jeder kritischen Einrichtung diesem Referenzniveau entspricht.

Ausgenommen davon können kritische Einrichtungen sein, deren wesentlicher Dienst auf einer netzförmigen, leitungsgebundenen oder räumlich weitverteilten Infrastruktur beruht, die eine Vielzahl physisch exponierter und nicht durchgehend sicherbarer Systembestandteile umfasst – insbesondere Leitungen, Trassen, Schächte, dezentrale Anlagen oder Übergabepunkte in öffentlichem Raum oder auf Liegenschaften Dritter. In solchen Fällen existiert eine Diskrepanz zwischen schützbaren und strukturell nicht sicherbaren Bereichen desselben Systems. Dies bedeutet, dass bei der Festlegung des Schutzniveaus für die schützbaren Bereiche die tatsächlich erreichbare Schutzwirkung für den wesentlichen Dienst durch die nicht sicherbaren Bereiche begrenzt wird.

Konkret bedeutet dies, dass der Schutzgewinn für den wesentlichen Dienst durch ein höheres Sicherungsniveau einzelner Objekte nicht im selben Maße proportional

zunimmt, solange Einwirkungsmöglichkeiten vergleichbarer Wirkung an nicht sicherbaren Stellen des Systems bestehen. Nichtsdestotrotz gibt es auch bei solchen kritischen Einrichtungen Anlagen und Knotenpunkte, die aufgrund ihrer Bedeutung für den wesentlichen Dienst oder ihrer Sichtbarkeit und Exponiertheit ungeachtet dessen eines besonderen Schutzes bedürfen – etwa weil sie als Steuerungs- oder Knotenpunkte eine systemübergreifende Funktion erfüllen, weil ihr Ausfall nicht durch Redundanzen kompensierbar ist oder weil sie als erkennbare kritische Infrastruktur ein erhöhtes Angriffsrisiko aufweisen.

Falls bei bestimmten netzförmigen Infrastrukturen die systemkritische Verwundbarkeit gerade in den strukturell nicht sicherbaren Bereichen liegt, ohne dass diese durch physische Schutzmaßnahmen oder ergänzende Maßnahmen im schützbaren Bereich wirksam kompensiert werden kann, ist dies im Schutzkonzept transparent auszuweisen. In diesem Fall kann es möglich sein, dass die die für die drei Risikoklassen – Klasse A, Klasse B und Klasse C – spezifischen Vorgaben, insbesondere in Bezug auf Einbruch- und Überfallmeldesysteme, Videoüberwachungs- und Zutrittssteuerungssysteme, in keinem einzigen Bereich vollinhaltlich zur Anwendung kommen.

Um die summierte mechanische Widerstandszeit aller physischen Schutzschichten auf die erforderliche Reaktionszeit abzustimmen, kann bei der Berechnung anstelle der reinen Widerstandszeit die maximale Gesamtprüfdauer – ein normativ definierter Wert, der zusätzlich Pausen und Werkzeugwechsel einschließt – als zeitlicher Widerstandswert der jeweiligen mechanischen Verschlüsse herangezogen werden. Sofern die ermittelte Reaktionszeit – insbesondere bei abgelegenen oder dislozierten Anlagen – strukturell nicht mit einem vertretbaren und verhältnismäßigen Aufwand zu den realisierbaren Widerstandswerten in Einklang gebracht werden kann, soll dies im Schutzkonzept nachvollziehbar dargelegt und begründet werden. In jedem Fall sollen aber geeignete kompensatorische Maßnahmen vorgesehen werden, die das verbleibende Risiko so weit wie möglich reduzieren.

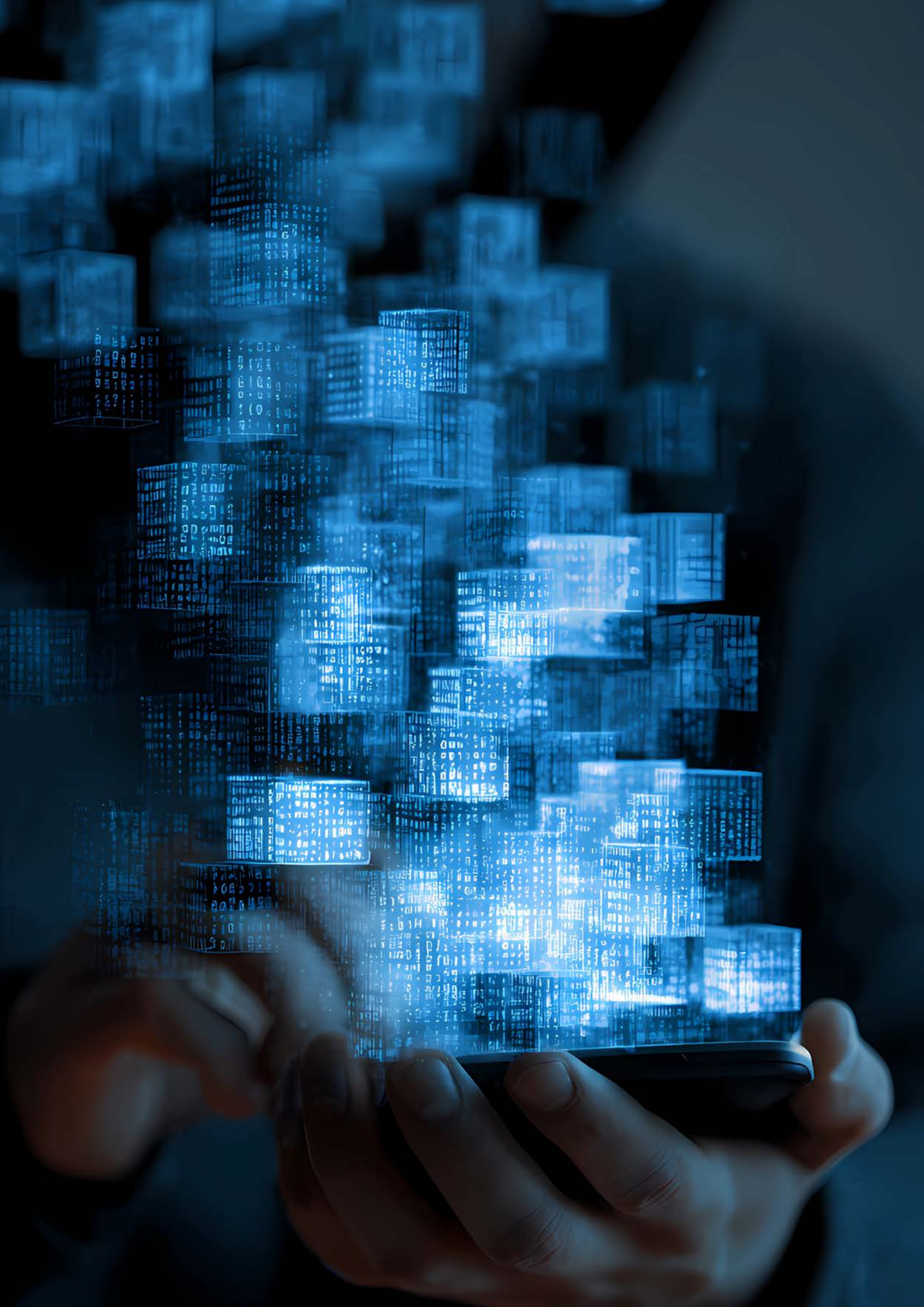
Alle widerstandsrelevanten Elemente sollen den Regeln der Technik entsprechen und Datenblätter sowie Nachweise über die Widerstandsklasse und relevante Eigenschaften sollen vorliegen. Zusätzlich soll der norm- und fachgerechte Einbau durch entsprechend qualifiziertes Personal dokumentiert werden, da andernfalls der Nachweis der Schutzwirkung nicht erbracht werden kann.

Die Schutzfunktion der eingesetzten Elemente soll dauerhaft aufrechterhalten werden. Die vorgeschriebenen Wartungszyklen sollen durch qualifizierte Fachkräfte eingehalten und sämtliche Wartungsmaßnahmen nachvollziehbar dokumentiert werden. Ergänzend dazu sollen Planung, Umsetzung und Betrieb von Ersatzmaßnahmen (Recovery) für den Fall des Ausfalls einzelner Komponenten oder ganzer Maßnahmenbereiche der physischen Sicherheit vorgesehen werden. Solche Ersatzmaßnahmen sollen unverzüglich ergriffen werden, damit durch den Ausfall keine Sicherheitslücken entstehen. Die Funktionsfähigkeit dieser Ersatzmaßnahmen soll regelmäßig überprüft und dokumentiert werden.

Wird aufgrund baulicher, betrieblicher oder wirtschaftlicher Restriktionen von den geforderten Konfigurationen abgewichen oder an relevanten Stellen andere bauliche, mechanische oder elektronische Komponenten anstelle normkonformer geprüfter Produkte eingesetzt, sind diese Abweichungen konkret zu benennen und sachlich zu begründen. Die alternativ erbrachte Schutzwirkung soll durch geeignete Nachweise (z.B. durch Sachverständige) attestiert werden.

7 Abschließende Vorgaben

Für die Umsetzung des Leitfadens Z 2 wird nochmals darauf hingewiesen, dass sämtliche Anforderungen auf den wesentlichen Dienst der kritischen Einrichtung bezogen sind. Die Resilienzmaßnahmen gemäß § 15 RKEG dienen nicht dem allgemeinen Schutz der Einrichtung als Unternehmen, sondern der Aufrechterhaltung der Fähigkeit, den wesentlichen Dienst zu erbringen. Ebenso sind die Grundsätze der Geeignetheit und Verhältnismäßigkeit, der Konformitätsvermutung einschließlich der Begründung bei Abweichungen, des Verhältnisses zu Normen und Richtlinien sowie der Stufenlogik der behördlichen Prüfung, wie in Leitfaden Z 0 dargelegt, zu beachten. Dem risikobasierten Ansatz folgend liegt die konkrete Ausgestaltung bei der kritischen Einrichtung selbst.



Z 3: Abwehr und Bewältigung von Sicherheitsvorfällen

1 Allgemeine Grundlagen

§ 15 Abs. 2 Z 3 RKEG sieht vor, dass kritische Einrichtungen geeignete und verhältnismäßige Maßnahmen zur Abwehr und Bewältigung von Sicherheitsvorfällen sowie zur möglichst weitgehenden Begrenzung ihrer Auswirkungen treffen. Diese Anforderung betrifft die Phase des eingetretenen oder sich konkret entwickelnden Vorfalls. Ziel ist es, die Handlungsfähigkeit der kritischen Einrichtung unter Störungsbedingungen sicherzustellen, eine Eskalation zu verhindern oder zu begrenzen sowie nachteilige Auswirkungen auf die Erbringung des wesentlichen Dienstes, auf Personen, Sachwerte, die Umwelt sowie auf verbundene Systeme und abhängige Leistungen zu reduzieren.

Die Anforderungen im vorliegenden Leitfaden Z 3 sind nicht auf einzelne Abwehrmaßnahmen im engeren Sinn beschränkt. Sie beziehen sich vielmehr auf die gesamte Reaktions-, Führungs-, Kommunikations- und Minderungsfähigkeit der kritischen Einrichtung im Sicherheitsvorfall. Erfasst sind technische und organisatorischeMaßnahmen, soweit sie der unmittelbaren Eindämmung eines Sicherheitsvorfalls, der Verlangsamung oder Verhinderung seiner Eskalation oder der Begrenzung seiner Folgen dienen.

Leitfaden Z 3 ist daher als systemische Anforderung zu verstehen. Maßgeblich ist nicht das bloße Vorhandensein einzelner Dokumente oder isolierter Maßnahmen, sondern ein belastbares und im Ereignisfall anwendbares System der Ereignisbewältigung.

Dieses System soll insbesondere umfassen:

- eine klare Aktivierungs- und Eskalationslogik sowie eine arbeitsfähige Führungsorganisation mit benannten Rollen, Befugnissen und Stellvertretungen,
- geregelte Lage- und Entscheidungsprozesse sowie belastbare Kommunikations- und Meldewege,
- definierte Schnittstellen zu Behörden, Einsatzorganisationen und sonstigen externen Stellen,
- technische sowie ressourcenbezogene Maßnahmen zur unmittelbaren Wirkungsminimierung.

Dabei gilt, dass kritische Einrichtungen angeregt werden, die folgenden Maßnahmen zur Abschwächung der Folgen von Sicherheitsvorfällen in Betracht zu ziehen:

- Kritische Einrichtungen sollen Maßnahmen vorsehen, um nachteilige Folgen eines Sicherheitsvorfalls auf das Umfeld – etwa Bevölkerung, Umwelt oder andere kritische Einrichtungen – zu begrenzen und die zuständigen Behörden so rasch zu informieren, dass diese unterstützend eingreifen können. Maßnahmen und Vorkehrungen zur Begrenzung nachteiliger Auswirkungen außerhalb des Standorts sowie zur raschen Benachrichtigung zuständiger Krisen- und Katastrophenschutzbehörden erfordern abgestimmte Verfahren, verlässliche Kommunikationskanäle und regelmäßige Übungen.
- Ebenso sollen Maßnahmen vorgesehen werden, um externe Unterstützung – etwa Feuerwehr, Rettungsdienste oder spezialisierte Hilfskräfte – wirksam in Reaktionsmaßnahmen vor Ort zu integrieren.

- Die Auslegung der Infrastruktur nach dem Prinzip „sicheres Versagen" bedeutet, sicherzustellen, dass eine Störung die Sicherheit von Personen nicht beeinträchtigt und kaskadierende Auswirkungen auf andere Bereiche abgeschwächt werden. Safe-to-fail-Merkmale ermöglichen es, während eines Ausfalls wesentliche Funktionen aufrechtzuerhalten oder kontrollierte Abschaltverfahren zu unterstützen, Geräteschäden zu verhindern und eine Wiederanlaufbarkeit sicherzustellen, sobald die Bedingungen dies zulassen.

Diese Grundsätze verdeutlichen, dass Z 3 nicht nur auf die unmittelbare Reaktion innerhalb der kritischen Einrichtung abzielt. Die Bestimmung umfasst vielmehr auch die Schnittstelle nach außen: die abgestimmte Zusammenarbeit mit Behörden und Unterstützungskräften, die Begrenzung von Auswirkungen außerhalb des Standorts sowie technische und betriebliche Vorkehrungen.

Resilienz ist, wie oben erwähnt, keine operative Einzelaufgabe, sondern eine Führungsverantwortung, die auf allen Ebenen der kritischen Einrichtung verankert sein muss. Kritische Einrichtungen sollen daher Resilienzziele festlegen und Strategie, Policy und Planung für Resilienz annehmen, diese den relevanten Interessenträgern gemäß dem Need-to-know-Prinzip kommunizieren und regelmäßig überprüfen. Dabei sollen bestehende Schwachstellen und Möglichkeiten berücksichtigt werden, wie Sicherheitsvorfälle besser verhindert, abgewehrt, bewältigt und ihre Auswirkungen begrenzt werden können.

2 Reaktions- und Führungsfähigkeit

Kritische Einrichtungen sollen sicherstellen, dass sie bei einem Sicherheitsvorfall rasch in einen strukturierten Führungsmodus wechseln können. Dafür sollen klare Aktivierungs- und Eskalationskriterien, geregelte Zuständigkeiten für die Erstbewertung, benannte Entscheidungsbefugnisse sowie nachvollziehbare Übergänge zwischen betrieblicher Störungsbearbeitung und übergeordneter Krisensteuerung vorgesehen werden. Ziel ist es, auch unter Zeitdruck, bei unvollständiger Informationslage und eingeschränkter Ressourcenverfügbarkeit entscheidungs- und handlungsfähig zu bleiben.

Die Führungsorganisation soll so ausgestaltet sein, dass Informationen rasch verdichtet, Lagebilder erstellt, Handlungsoptionen bewertet und Maßnahmen priorisiert werden können. Soweit Größe, Komplexität und Vernetzung der kritischen Einrichtung dies erfordern, soll zwischen strategischer Entscheidung, koordinierender Lageführung und operativer Umsetzung unterschieden werden. Ein kurz gefasster, szenarienunabhängiger Krisenmanagementplan mit klaren Rollen, Abläufen und Vorlagen ist dafür ein wesentliches Instrument. Resilienz soll dabei nicht nur als Einzelmaßnahme, sondern als strukturell verankerte Führungsaufgabe verstanden werden; angemessene Resilienzkompetenz wird auf Ebene der obersten Leitung sowie in Resilienz- oder Risikomanagementfunktionen gebündelt, um eine ausreichende strategische und operative Resilienzplanung sicherzustellen.

Zur Führungskompetenz gehört auch die Fähigkeit, vorab festzulegen, welche Funktionen, Prozesse und Leistungen bei einem Sicherheitsvorfall prioritär aufrechtzuerhalten oder in einen reduzierten Betriebsmodus zu überführen sind. Dazu sollen abgestufte Handlungsoptionen vorgesehen werden, mit denen auf unterschiedliche Schweregrade und Entwicklungen eines Vorfalls reagiert werden kann. Die Lage- und Entscheidungsprozesse sollen nicht auf maximale Informationssammlung, sondern auf belastbare Entscheidungsfähigkeit ausgerichtet sein; klar geregelte Verfahren für Lagebewertung, Prioritätensetzung und Maßnahmensteuerung sollen sicherstellen, dass auch unter Zeitdruck handlungsleitend entschieden werden kann.

Aktivierung und Eskalation sollen auf vorab festgelegten Kriterien beruhen. Dazu zählen definierte Auslöser, Schwellenwerte oder Lageindikatoren, klare Befugnisse zur Aktivierung der Führungsorganisation, festgelegte Eskalationsstufen sowie nachvollziehbare Rücknahme- und Deeskalationskriterien. Ein Lagebild soll die wesentlichen Informationen zu Betroffenheit, Risiken, eingeleiteten Maßnahmen, offenen Handlungsbedarfen und erwartbaren Entwicklungen in kompakter, entscheidungsbezogener Form zusammenführen. Entscheidungen und wesentliche Begründungen sollen fortlaufend dokumentiert werden, um Führungsstabilität, Nachvollziehbarkeit und geordnete Übergaben sicherzustellen.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖNORM EN ISO 22361	Sicherheit und Resilienz – Krisenmanagement – Leitlinien (Kap. 5.2; Kap. 5.3.4; Kap. 6; Kap. 8; Kap. 9)
DIN ISO 22320	Sicherheit und Resilienz – Gefahrenabwehr – Leitfaden für die Organisation der Gefahrenabwehr bei Schadensereignissen (Kap. 4; Kap. 5; Kap. 6)
ÖNORM D 4902-3	Risikomanagement für Organisationen und Systeme – Leitfaden – Teil 3: Notfall-, Krisen- und Kontinuitätsmanagement – Anleitung zur Umsetzung der ISO 31000

Stand: 01. Juni 2026

Tipps

Aktivierungs- und Eskalationskriterien sollen so formuliert sein, dass sie auch unter Zeitdruck ohne Interpretationsspielraum anwendbar sind. Zu komplexe Eskalationsmodelle verzögern häufig die Reaktionsfähigkeit.
Was nicht geübt wird, steht im Ernstfall nicht verlässlich zur Verfügung. Dabei ist vorab zu klären, welche Pläne an externe Stellen weitergegeben werden können. Ein einfacher, nicht klassifizierter Plan mit klaren Kontaktpunkten ist für die Zusammenarbeit vor Ort oft wirksamer als ein detailliertes, aber vertrauliches Dokument.

3 Kommunikation und externe Schnittstellen

Kritische Einrichtungen sollen sicherstellen, dass im Zuge von Sicherheitsvorfällen verlässliche interne und externe Kommunikationswege sowie klar geregelte Schnittstellen zu relevanten Stellen vorhanden sind. Ziel ist es, Informationen zeitgerecht, konsistent und adressatengerecht weiterzugeben, Entscheidungen abzustimmen, Unterstützungsleistungen rasch einzubinden und Fehlentwicklungen durch verspätete, unvollständige oder widersprüchliche Kommunikation zu vermeiden. Kommunikationsfähigkeit ist damit ein wesentlicher Bestandteil dieser Ereignisbewältigung – nicht nur als technische Übermittlungsfunktion, sondern als Führungs- und Koordinationsaufgabe.

Die Kommunikationsorganisation soll so ausgestaltet sein, dass interne Alarmierung, Lagekommunikation, externe Meldungen und koordinierte Abstimmungen auch unter Bedingungen eines Sicherheitsvorfalls aufrechterhalten werden können. Dafür sollen insbesondere interne Alarmierungs- und Erreichbarkeitsregelungen, definierte Meldewege an zuständige Stellen, klare Zuständigkeiten für externe Kommunikation, vorbereitete Kommunikationsmittel und Vorlagen sowie Ausweichlösungen bei Ausfall regulärer Kommunikationskanäle vorgesehen werden. Soweit Größe, Komplexität und Vernetzung der kritischen Einrichtung dies erfordern, sollen Kommunikationsaufgaben innerhalb der Führungsorganisation klar zugeordnet und von allgemeinen operativen Tätigkeiten abgegrenzt werden.

Kritische Einrichtungen sollen sicherstellen, dass Ansprechpartnerinnen/Ansprechpartner, Kontaktpunkte, Meldeverfahren und Eskalationsmechanismen gegenüber Behörden, Einsatzorganisationen, Dienstleistern und sonstigen Unterstützungsstellen vorbereitet und dokumentiert sind. Externe Kommunikation in Krisenlagen erfolgt häufig unter hoher Dynamik und Unsicherheit; sie soll daher auf vorab festgelegten Zuständigkeiten, Freigaben und Prioritäten beruhen. Für Vorfälle mit Auswirkungen außerhalb des Standorts sollen Maßnahmen und Vorkehrungen zur Begrenzung nachteiliger Auswirkungen außerhalb des Standorts sowie zur raschen Benachrichtigung zuständiger Krisen- und Katastrophenschutzbehörden vorgesehen werden, gestützt auf abgestimmte Verfahren, verlässliche Kommunikationskanäle und regelmäßige Übungen. Ebenso soll die Fähigkeit bestehen, externe Unterstützung wirksam in Reaktionsmaßnahmen vor Ort zu integrieren.

Die Zusammenarbeit mit externen Stellen soll nicht erst im Ereignisfall anlaufen, sondern strukturell vorbereitet sein. Das erfordert laufende Absprachen mit zuständigen Behörden und Einsatzorganisationen.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖNORM EN ISO 22361	Sicherheit und Resilienz – Krisenmanagement – Leitlinien (Kap. 5.3.4; Kap. 6; Kap. 7; Kap. 9)
DIN ISO 22320	Sicherheit und Resilienz – Gefahrenabwehr – Leitfaden für die Organisation der Gefahrenabwehr bei Schadensereignissen (Kap. 4; Kap. 5; Kap. 6)
ÖNORM D 4902-3	Risikomanagement für Organisationen und Systeme – Leitfaden – Teil 3: Notfall-, Krisen- und Kontinuitäts-management – Anleitung zur Umsetzung der ISO 31000

Stand: 01. Juni 2026

Tipps

Kommunikationswege sollen nicht nur dokumentiert, sondern regelmäßig praktisch getestet werden. Kontaktlisten, Freigaben und Meldewege, die in der Theorie klar erscheinen, erweisen sich in dynamischen Lagen häufig als unzureichend.
Für Erstmeldungen, Lage-Updates und Unterstützungsanforderungen sollen einfache standardisierte Vorlagen vorgesehen werden, damit Informationen rasch, vollständig und vergleichbar übermittelt werden können.
Zuständigkeiten für externe Kommunikation sollen frühzeitig eindeutig festgelegt werden – unklare Sprecherrollen oder parallele Kommunikationswege erhöhen das Risiko widersprüchlicher Aussagen und erschweren die Koordination mit Behörden und externen Partnern.

4 Technische Wirkungsminimierung

Die im vorliegenden Leitfaden Z 3, Kapitel 1 beschriebenen Grundsätze zur sicheren Infrastrukturauslegung sind durch konkrete technische Vorkehrungen zu hinterlegen. Technische Wirkungsminimierung umfasst den Aufbau von Redundanzen sowie Härtung. Dies soll Backup-Systeme mit Spezifikationen zu Funktion, Dauer und Priorität der Wiederaufnahme inkludieren. Dabei soll auch die Integrität von IT-Netzen und -Systemen sowie von in Anlagen eingesetzter Software berücksichtigt werden, insbesondere im Hinblick auf eine übermäßige Abhängigkeit von Hochrisiko-Lieferanten.

Technische Vorkehrungen sollen auf die Begrenzung von Sekundärschäden und Kaskadeneffekten auf Systemebene ausgerichtet sein. Maßnahmen sollen die Ausbreitung technischer Störungen auf andere Anlagenteile oder Systeme verhindern, die Stabilität kritischer Teilfunktionen sichern und den Übergang in definierte technische Notbetriebszustände ermöglichen – auch für länger andauernde Lagen, in denen kritische Infrastruktur oder externe Unterstützung nur eingeschränkt verfügbar sind.
Im Bereich der Energieabsicherung sollen alternative Stromversorgungssysteme

berücksichtigt werden – etwa Generatoren und Batterien für unterbrechungsfreie Stromversorgung. Backup-Systeme sollen regelmäßig getestet werden, wobei auf eine Kraftstoff-Autonomie von zumindest 72 Stunden sowie auf aktivierbare Lieferantenverträge für Notfallunterstützung, Lieferung, Einsätze und Reparaturen geachtet werden soll.

Technische Maßnahmen sollen auch nicht isoliert betrachtet werden. Ihre Wirksamkeit entfaltet sich erst im Zusammenspiel mit Aktivierung, Lageführung, Kommunikation und Ressourcensteuerung.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖNORM EN ISO 22361	Sicherheit und Resilienz – Krisenmanagement – Leitlinien (Kap. 5.3.4; Kap. 6; Kap. 7; Kap. 9)
DIN ISO 22320	Sicherheit und Resilienz – Gefahrenabwehr – Leitfaden für die Organisation der Gefahrenabwehr bei Schadensereignissen (Kap. 4; Kap. 5; Kap. 6)
ÖNORM D 4902-3	Risikomanagement für Organisationen und Systeme – Leitfaden – Teil 3: Notfall-, Krisen- und Kontinuitätsmanagement – Anleitung zur Umsetzung der ISO 31000

Stand: 01. Juni 2026

Tipps

Technische Schutzmaßnahmen sollen nicht nur für den Regelbetrieb, sondern ausdrücklich für Sicherheitsvorfälle und kontrollierte Abschaltungen ausgelegt werden. Es soll frühzeitig geprüft werden, welche Funktionen im Fall eines Ausfalls zwingend technisch abgesichert sein müssen, welche Zustände kontrolliert erreicht werden sollen und welche Systeme für einen sicheren Wiederanlauf verfügbar bleiben müssen.
Bei Ersatzversorgung und Backup-Systemen sollen nicht nur technische Komponenten, sondern auch Kraftstoff, Wartung, Ersatzteile, Bedienbarkeit und externe Unterstützungsleistungen berücksichtigt werden.
Gefährliche Stoffe, temperaturkritische Anlagen und personalrelevante Bereiche sollen in technischen Notfallkonzepten gesondert betrachtet werden, da hier häufig die höchsten Folgewirkungen und Kaskadenrisiken entstehen.

5 Ressourcenbezogene Wirkungsminimierung

Ressourcenbezogene Wirkungsminimierung umfasst jene Vorsorgemaßnahmen, die es kritischen Einrichtungen ermöglichen, auch unter Bedingungen eines Sicherheitsvorfalls wesentliche Mindestfunktionen aufrechtzuerhalten, kritische Engpässe zu bewältigen und die Ausweitung eines Sicherheitsvorfalls durch Ausfall oder Mangel zentraler Ressourcen zu verhindern. Im Unterschied zur technischen Wirkungsminimierung richtet sich der Fokus nicht nur auf kritische Infrastrukturen, sondern auch auf Ressourcen und Versorgungsgrundlagen, die für deren Betrieb unter den Bedingungen eines Sicherheitsvorfalls zwingend verfügbar bleiben müssen.

Kritische Einrichtungen sollen vorab festlegen, welche Funktionen, Betriebsmittel, Medien, Stoffe, Komponenten, Personal und Unterstützungsleistungen bei einem Sicherheitsvorfall prioritär verfügbar bleiben müssen. Dazu sollen kritische Ressourcen und Abhängigkeiten identifiziert, nach ihrer Bedeutung für den wesentlichen Dienst bewertet und mit risikobasierten Maßnahmen abgesichert werden. Kritische Einrichtungen sollen dabei den Versorgungsbedarf klar definieren und Bezugsquellen durch alternative Anbieter und Routen diversifizieren. Dies gilt insbesondere dort, wo der Ausfall einzelner Ressourcen zu rascher Eskalation, schwerwiegenden Zusatzfolgen oder zur Beeinträchtigung anderer Schutzgüter führen kann.

Ein besonderer Schwerpunkt soll auf Ausweichversorgung und alternativen Quellen während eines Sicherheitsvorfalles liegen. Für die Wasserversorgung können kritische Einrichtungen während Störungen die Nutzung auf kritische Funktionen beschränken und alternative Quellen einsetzen, darunter Reservebrunnen, Speichertanks, mobile Aufbereitungseinheiten und flexible Speicheroptionen. Kritische Einrichtungen im Trinkwassersektor sollen darüber hinaus Notversorgungspunkte definieren. Für andere sektorspezifische Versorgungsbedarfe soll die Notfallplanung in der Lieferkette eine Verlagerung von „just-in-time" zu „just-in-case"-Bestandsplanungsmodellen in Betracht ziehen, wo dies angemessen ist. Ausweichsysteme sollen vorab vereinbarte Backup-Ressourcen und Sicherheits- bzw. Notfallbestände umfassen.

Zur ressourcenbezogenen Wirkungsminimierung gehört auch die Fähigkeit, kritische Wartungs- und Reparaturleistungen unter den Bedingungen eines Sicherheitsvorfalls sicherzustellen. Kritische Einrichtungen sollen umfassende Wartungsprogramme auf Basis von Herstellerempfehlungen, Betriebserfahrung und spezifischer Risikoanalyse entwickeln. Für die Reaktion auf Überwachungssystemwarnungen sollen klare Protokolle festgelegt werden, die die Überprüfung von Warnungen, die Beurteilung der Dringlichkeit und die Mobilisierung von Wartungsressourcen sowie Eskalationsverfahren für Situationen, die sofortige Aufmerksamkeit erfordern, umfassen.

Auch ressourcenbezogene Maßnahmen entfalten ihre Wirksamkeit erst im Zusammenspiel mit Reaktions- und Führungsfähigkeit, Kommunikation und technischen Notfallmaßnahmen; sie sind daher integraler Bestandteil des Gesamtsystems der Ereignisbewältigung.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖNORM EN ISO 22361	Sicherheit und Resilienz – Krisenmanagement – Leitlinien (Kap. 5.3.4; Kap. 6; Kap. 7; Kap. 9)
DIN ISO 22320	Sicherheit und Resilienz – Gefahrenabwehr – Leitfaden für die Organisation der Gefahrenabwehr bei Schadensereignissen (Kap. 4; Kap. 5; Kap. 6)
ÖNORM D 4902-3	Risikomanagement für Organisationen und Systeme – Leitfaden – Teil 3: Notfall-, Krisen- und Kontinuitätsmanagement – Anleitung zur Umsetzung der ISO 31000

Stand: 01. Juni 2026

Tipps

Es soll vorab festgelegt werden, welche Ressourcen für die Aufrechterhaltung wesentlicher Mindestfunktionen zwingend erforderlich sind und welche Alternativen oder Reserven für einen begrenzten Zeitraum verfügbar sein müssen.
Kritische Ressourcen sollen nicht nur identifiziert, sondern auch in ihrer tatsächlichen Verfügbarkeit unter Bedingungen eines Sicherheitsvorfalls bewertet werden. Lieferzeiten, Substitutionsmöglichkeiten, Mindestbestände und externe Abhängigkeiten sind dabei maßgeblich.
Bei Ersatzversorgung und Sicherheitsreserven sollen nicht nur technische Komponenten, sondern auch Verbrauchsmaterialien, Kraftstoff, Chemikalien, Ersatzteile, Personalverfügbarkeit und externe Unterstützungsleistungen berücksichtigt werden.

6 Dokumentation, Übung und Verbesserung

Die Anforderungen nach Leitfaden Z 3 sollen dokumentiert, nachvollziehbar und überprüfbar umgesetzt werden. Nachweisbar sein sollen insbesondere die Führungsorganisation, Rollen und Stellvertretungen, Aktivierungs- und Eskalationskriterien, Krisenmanagement- und Kommunikationsdokumente, Meldewege, Verfahren zur Priorisierung von Funktionen und Ressourcen sowie technische, betriebliche und ressourcenbezogene Maßnahmen zur Wirkungsminimierung. Die Dokumentation soll dabei nicht nur der späteren Überprüfung dienen, sondern auch als Führungs-, Steuerungs- und Entscheidungsgrundlage bei einem Sicherheitsvorfall nutzbar sein. Die bestehende Ausarbeitung zu Leitfaden Z 3 ordnet Dokumentation, Übung und Verbesserung bereits ausdrücklich als integralen Bestandteil eines belastbaren Systems der Ereignisbewältigung ein.

Zur Nachvollziehbarkeit und Wirksamkeit der Maßnahmen sollen Verfahren zur fortlaufenden Dokumentation von Lage, Entscheidungen und Maßnahmen bei einem Sicherheitsvorfall vorgesehen werden. Dies soll insbesondere sicherstellen, dass

Führungsentscheidungen, Zustandsänderungen, Priorisierungen, externe Abstimmungen und eingeleitete Maßnahmen auch bei längeren oder dynamischen Lagen konsistent nachvollzogen, übergeben und ausgewertet werden können. Die Dokumentation soll damit nicht als rein formaler Akt, sondern als Bestandteil geordneter Lagebearbeitung verstanden werden.

Übungen sollen ein zentrales Element der Wirksamkeitsprüfung und Weiterentwicklung der Maßnahmen nach Leitfaden Z 3 sein. Für die Begrenzung nachteiliger Auswirkungen außerhalb des Standorts sollen abgestimmte Verfahren, verlässliche Kommunikationskanäle und regelmäßige Krisen- und Katastrophenschutzübungen vorgesehen werden. Daraus soll folgen, dass insbesondere Führungs-, Kommunikations-, Melde- und Schnittstellenprozesse nicht nur dokumentiert, sondern regelmäßig praktisch erprobt werden sollen. Dies umfasst sowohl interne Abläufe als auch die Zusammenarbeit mit Behörden, Einsatzorganisationen und sonstigen Unterstützungsstellen.

Übungen und Überprüfungen sollen nicht auf Alarmierungs- oder Erreichbarkeitstests beschränkt bleiben. Sie sollen vielmehr auch die Aktivierung der Führungsorganisation, die Lage- und Entscheidungsprozesse, die Einbindung externer Stellen, die Anwendung von Minderungsmaßnahmen sowie die Handhabung von Ausweich- und Ersatzlösungen umfassen. Sofern Vorfälle über den Standort hinausgehen, sollen auch diese Auswirkungen in Übungen und Reviews berücksichtigt werden. Gleiches soll für Szenarien mit Ressourcenengpässen, technischen Ausfällen, Kommunikationsstörungen oder längerer Einsatzdauer gelten.

Gewonnene Erkenntnisse aus Übungen und Sicherheitsvorfällen sollen systematisch ausgewertet und in Verbesserungsmaßnahmen überführt werden. Dies soll sowohl für tatsächliche Sicherheitsvorfälle als auch für Übungen, Beinahe-Sicherheitsvorfälle und sonstige relevante Erkenntnisquellen gelten. Ziel soll es sein, Schwachstellen frühzeitig zu erkennen, Maßnahmen zu präzisieren, Rollen und Abläufe nachzuschärfen sowie Verfahren, Ressourcen und Unterstützungsstrukturen fortlaufend an veränderte Rahmenbedingungen anzupassen. Dokumentation, Übung und Verbesserung sollen damit als zusammenhängender Zyklus verstanden werden.

Für die Ausgestaltung von Dokumentation, Übung und Verbesserung sollen einschlägige internationale, europäische und nationale Normen und Richtlinien zum Krisen-, Notfall- und Kontinuitätsmanagement herangezogen werden. Die Normen und Richtlinien sollen insbesondere dort Orientierung geben, wo es um Validierung, Auswertung, Verbesserungsmaßnahmen, Training, Rollenklärung und die laufende Weiterentwicklung der Ereignisbewältigungsfähigkeit geht. Der Leitfaden Z 3 verweist bereits auf die Bedeutung regelmäßiger Übungen, Reviews und der strukturierten Überführung von gewonnenen Erkenntnissen in Verbesserungsmaßnahmen.

Dokumentation, Übung und Verbesserung sollen nicht isoliert als nachgelagerte Qualitätssicherung verstanden werden. Sie sollen vielmehr Bestandteil des Gesamtsystems sein, mit dem kritische Einrichtungen ihre Reaktions-, Führungs-, Kommunikations- und Minderungsfähigkeit belastbar machen, überprüfen und laufend

weiterentwickeln. Nur geübte, dokumentierte und fortgeschriebene Verfahren können bei einem Sicherheitsvorfall tatsächlich belastbar sein.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖNORM EN ISO 22361	Sicherheit und Resilienz – Krisenmanagement – Leitlinien (Kap. 5.3.4; Kap. 6; Kap. 9)
DIN ISO 22320	Sicherheit und Resilienz - Gefahrenabwehr – Leitfaden für die Organisation der Gefahrenabwehr bei Schadensereignissen (Kap. 5; Kap. 6)
ISO 22398	Societal security – Guidelines for exercises (Kap. 4; Kap. 5; Kap. 6)
ÖNORM D 4902-3	Risikomanagement für Organisationen und Systeme – Leitfaden – Teil 3: Notfall-, Krisen- und Kontinuitäts-management – Anleitung zur Umsetzung der ISO 31000

Stand: 01. Juni 2026

Tipps

Die Dokumentation soll im Ereignisfall so einfach wie möglich und so strukturiert wie nötig sein. Zu umfangreiche Dokumentationsvorgaben werden in dynamischen Lagen häufig nicht durchgehalten.

Es soll vorab festgelegt werden, welche Lageinformationen, Entscheidungen und Maßnahmen jedenfalls dokumentiert werden müssen und wer dafür verantwortlich ist. Übungen sollen nicht nur einzelne Teilaspekte, sondern regelmäßig auch das Zusammenwirken von Führung, Kommunikation, Schnittstellen und Minderungs-maßnahmen abbilden.

Übungen sollen möglichst realitätsnah gestaltet und an den tatsächlichen Risiken, Abhängigkeiten und Rahmenbedingungen der jeweiligen kritischen Einrichtung ausgerichtet werden. Zu abstrakte oder stark schematisierte Szenarien sind nur eingeschränkt geeignet, um Führungs-, Entscheidungs- und Kommunikationsfähig-keit belastbar zu überprüfen.

Szenarien sollen fachlich plausibel und in ihrer Dynamik realistisch ausgestaltet sein. Dazu sollen insbesondere Zeitdruck, unvollständige Informationen, Ziel-konflikte, Mehrfachbelastungen, Kommunikationsstörungen und externe Einflüsse berücksichtigt werden.

Immersive Übungsformen sollen dort genutzt werden, wo Führungsarbeit, Kommunikation und Entscheidungsfähigkeit unter möglichst realitätsnahen Bedingungen überprüft werden sollen. Geeignet sind insbesondere realitätsnahe Einspielungen, abgestufte Lageentwicklungen, externe Rückmeldungen, Behörden-anfragen oder simulierte Medien- und Stakeholder-Lagen.

Bei komplexeren Übungen soll die Einbindung externer Personen für Training, Übungsleitung oder Beobachtung geprüft werden. Externe Perspektiven können

dazu beitragen, die Übungsdurchführung konsistent zu steuern, organisationsinterne blinde Flecken sichtbar zu machen und die Auswertung methodisch zu stärken.
Die Evaluierung soll bereits in der Planungsphase mitgedacht werden. Es soll vorab festgelegt werden, welche Übungsziele verfolgt, welche Beobachtungsschwerpunkte gesetzt und anhand welcher Kriterien Führungs-, Kommunikations-, Schnittstellen- und Minderungsmaßnahmen beurteilt werden sollen.
Nach Übungen soll zeitnah eine strukturierte Nachbesprechung erfolgen. Beobachtungen, Schwachstellen, funktionierende Elemente und Verbesserungsbedarfe sollen gesichert und in konkrete Maßnahmen mit klaren Verantwortlichkeiten und Umsetzungsfristen überführt werden.
Gewonnene Erkenntnisse sollen nachvollziehbar in Verfahren, Vorlagen, Rollen, Ressourcenplanung und weitere Schulungs- und Übungsmaßnahmen einfließen. Nur dadurch entsteht aus Übungen ein nachhaltiger Mehrwert für die Krisen- und Resilienzfähigkeit der kritischen Einrichtung.

7 Abschließende Vorgaben

Für die Umsetzung des Leitfadens Z 3 wird nochmals darauf hingewiesen, dass sämtliche Anforderungen auf den wesentlichen Dienst der kritischen Einrichtung bezogen sind. Die Resilienzmaßnahmen gemäß RKEG § 15 dienen nicht dem allgemeinen Schutz der Einrichtung als Unternehmen, sondern der Aufrechterhaltung der Fähigkeit, den wesentlichen Dienst zu erbringen. Ebenso sind die Grundsätze der Geeignetheit und Verhältnismäßigkeit, der Konformitätsvermutung einschließlich der Begründung bei Abweichungen, des Verhältnisses zu Normen und Richtlinien sowie der Stufenlogik der behördlichen Prüfung, wie im Leitfaden Z 0 dargelegt, zu beachten. Dem risikobasierten Ansatz folgend liegt die konkrete Ausgestaltung bei der kritischen Einrichtung selbst.

Die Resilienz- und Schutzfunktion der vorgesehenen Maßnahmen soll dauerhaft aufrechterhalten werden. Übungen sind entscheidend für die Validierung des Resilienzplans einer kritischen Einrichtung und dafür, dass das Personal seine Rollen im Ernstfall wirksam wahrnehmen kann. Dabei sollen kritische Einrichtungen den Fokus auf die Ergebnisse ihrer einrichtungsinternen Risikoanalyse legen, den vollständigen Resilienzkreislauf testen und eine gute sektorübergreifende Koordination sicherstellen. Ebenso soll die Zusammenarbeit mit zuständigen Behörden (wie Strafverfolgung) sowie Einsatzorganisationen (wie Feuerwehr und Rettungsdiensten) sichergestellt und diese in Übungen einbezogen werden. Soweit Wartung, Überprüfung, Aktualisierung oder sonstige wiederkehrende Maßnahmen erforderlich sind, sollen diese verbindlich vorgesehen und nachvollziehbar dokumentiert werden.

Z 4: Fortführung und Wiederaufnahme nach Sicherheitsvorfällen

1 Allgemeine Grundlagen

Kritische Einrichtungen haben geeignete und verhältnismäßige Resilienzmaßnahmen zu treffen, um nach Sicherheitsvorfällen die Fortsetzung oder rasche Wiederaufnahme des wesentlichen Dienstes zu gewährleisten. Die Anforderung betrifft die Phase der Stabilisierung, Wiederaufnahme und geordneten Rückführung in einen belastbaren Betriebszustand. Ziel ist es, die Erbringung des wesentlichen Dienstes auch nach erheblichen Störungen zu sichern, Mindestleistungsniveaus aufrechtzuerhalten oder die Wiederaufnahme in vertretbarer Zeit zu ermöglichen.

Die Anforderung setzt dort an, wo die akute Bewältigung eines Sicherheitsvorfalls in die gezielte Wiederaufnahme übergeht. Während die Abwehr, Bewältigung und Wirkungsminimierung darauf ausgerichtet ist, einen Sicherheitsvorfall einzudämmen und seine unmittelbaren Auswirkungen zu begrenzen, richtet sich die Fortsetzung und Wiederaufnahme auf die strukturierte Rückführung der wesentlichen Dienste: von der Aufrechterhaltung priorisierter Mindestleistungen über die schrittweise Wiederaufnahme kritischer Funktionen bis zur kontrollierten Rückkehr in den Regelbetrieb. Beide Phasen greifen ineinander, erfordern jedoch unterschiedliche Planungs-, Steuerungs- und Entscheidungslogiken.

Die Anforderungen sind nicht auf die bloße Wiederaufnahme einzelner Anlagen, Systeme oder Prozesse beschränkt. Sie beziehen sich vielmehr auf die gesamte Kontinuitäts- und Wiederaufnahmefähigkeit der kritischen Einrichtung. Maßgeblich ist nicht das bloße Vorhandensein einzelner Notfall- oder Wiederaufnahmemaßnahmen, sondern ein belastbares und im Störungsfall anwendbares System der Kontinuität und Wiederaufnahme.

Dieses System soll insbesondere umfassen:

- eine priorisierte Fortführung wesentlicher Leistungen auf Basis vorab definierter Mindestleistungsniveaus und kritischer Funktionen,
- die rasche Wiederaufnahme kritischer Teilleistungen durch vorbereitete Wiederanlauf- und Wiederherstellungsverfahren,
- die Verfügbarkeit erforderlicher Ressourcen, Redundanzen und alternativer Lösungen,
- die kontrollierte Rückkehr in den Regelbetrieb einschließlich Validierung, Freigabe und Kommunikation.

Resilienz ist, wie oben erwähnt, keine operative Einzelaufgabe, sondern eine Führungsverantwortung, die auf allen Ebenen der Einrichtung verankert sein soll. Kritische Einrichtungen sollen daher Resilienzziele festlegen und Strategie, Policy und Planung für Resilienz annehmen, diese den relevanten Interessenträgern gemäß dem Need-to-know-Prinzip kommunizieren und regelmäßig überprüfen. Dabei sollen bestehende Schwachstellen und Möglichkeiten berücksichtigt werden, wie Sicherheitsvorfälle besser verhindert, abgewehrt, bewältigt und ihre Auswirkungen begrenzt werden können. Kritische Einrichtungen sollen prüfen, ob die Bündelung angemessener Resilienzkompetenz auf Ebene der obersten Leitung sowie in Resilienz- oder

Risikomanagementfunktionen sinnvoll ist und ob die Bestellung eines Resilienzbeauftragten in Betracht gezogen werden soll, der die koordinierenden Rollen und Zuständigkeiten für die Umsetzung der Resilienzziele klar bündelt.

Darüber hinaus sollen die kritischen Einrichtungen auch in der Phase der Wiederaufnahme die Zusammenarbeit mit den politischen Entscheidungsträgern sowie zuständigen Behörden und Einsatzorganisationen etablieren und formalisieren, wie zum Beispiel mit Strafverfolgungsbehörden, Rettungsdiensten oder Landesverteidigung.

Vernetzend mit der NIS-2-Richtlinie ist festzuhalten, dass Maßnahmen zur Sicherstellung der Kontinuität und Wiederherstellung des wesentlichen Dienstes die Verpflichtungen zum Cybersicherheits-Risikomanagement unberührt lassen. Bestehende Maßnahmen aus diesem Bereich sollen, soweit möglich, integriert und nicht parallel aufgebaut werden.

2 Mindestleistungen, Priorisierung und Wiederanlaufsteuerung

Kritische Einrichtungen sollen sicherstellen, dass die wesentlichen Dienste auch unter Störungsbedingungen in einem definierten Mindestumfang fortgesetzt oder nach einem Sicherheitsvorfall in einer nachvollziehbaren Reihenfolge wiederhergestellt werden können. Dafür sollen kritische Funktionen, prioritäre Teilleistungen und erforderliche Mindestleistungsniveaus vorab bestimmt werden. Maßgeblich ist dabei nicht die technische Wiederherstellbarkeit einzelner Systeme, sondern die Frage, welche Funktionen und Leistungen zuerst verfügbar sein müssen, damit der wesentliche Dienst in einem tragfähigen Umfang erbracht werden kann. Ziel ist es, bei eingeschränkter Verfügbarkeit von Ressourcen, Personal, Infrastruktur oder Lieferungen jene Leistungen vorrangig aufrechtzuerhalten oder wiederaufzunehmen, die für die Erbringung des wesentlichen Dienstes besonders bedeutsam sind.

Dabei soll berücksichtigt werden, dass sich die Priorisierung nicht nur auf interne Prozesse, sondern auch auf deren Abhängigkeiten erstrecken soll. Dies betrifft insbesondere Personal, IT- und OT-Systeme, Energieversorgung, Kommunikationsmittel, Gebäude, externe Dienstleistungen, Transport, Rohstoffe, Hilfsstoffe, Ersatzteile und lieferkettenbezogene Unterstützungsleistungen. Mindestleistungen sollen daher nicht abstrakt, sondern in Verbindung mit den jeweils dafür erforderlichen Ressourcen, Schnittstellen und Voraussetzungen definiert werden.

In diesem Zusammenhang sollen kritische Einrichtungen ermitteln, welche spezifischen Teilleistungen am kritischsten sind, sodass sie zuerst wiederaufgenommen werden (Priorisierung von Diensten). Dabei soll unter anderem in Betracht gezogen werden, Hardware manuell zu betreiben, falls automatisierte oder KI-gestützte Systeme ausfallen oder manipuliert werden. Weiters sollen immer ausreichende personelle Ressourcen sichergestellt werden.

Mindestleistungen und Prioritäten sollen in eine strukturierte Wiederanlaufsteuerung eingebettet werden. Diese soll klare Aktivierungskriterien, geregelte Zuständigkeiten, definierte Freigabepunkte und nachvollziehbare Übergänge zwischen Reaktion, Wiederherstellung, Wiederaufnahme und Rückkehr in den Normalbetrieb vorsehen. Kritische Einrichtungen sollen daher vorab festlegen, wer Wiederherstellungsentscheidungen trifft, auf welcher Grundlage priorisiert wird, welche Funktionen zuerst wiederhergestellt werden sollen und unter welchen Voraussetzungen ein Übergang in die nächste Phase erfolgen kann.

Die Wiederanlaufsteuerung soll phasenweise aufgebaut sein. Kritische Einrichtungen sollen dafür abgestufte Wiederanlaufprotokolle umsetzen, die die Wiederaufnahme kritischer Funktionen auf Grundlage der Ergebnisse der Business Impact Analyse priorisieren. Diese Protokolle sollen systematische Validierungsverfahren für kritische Systeme, umfassende Tests der Datenintegrität und Funktionalität, Qualitätskontrollmaßnahmen sowie einen kontrollierten Übergang vom Notfall- zum Normalbetrieb durch schrittweise Kapazitätserhöhungen und Leistungsmonitoring umfassen. Kritische Funktionen und besonders auswirkungsrelevante Teilleistungen sollen zuerst adressiert werden. Anschließend sollen weitere Systeme, Prozesse oder Leistungen kontrolliert zugeschaltet, geprüft und stabilisiert werden. Ziel ist ein geordneter Übergang in einen belastbaren Betriebszustand; ungeprüfte oder unkoordinierte Wiederanläufe sollen vermieden werden.

Aktivierungs- und Wiederanlaufkriterien sollen auf vorab festgelegten Verfahren beruhen. Dazu sollen insbesondere definierte Mindestleistungsniveaus, priorisierte Wiederaufnahmereihenfolgen, klare Entscheidungsbefugnisse, dokumentierte Freigabeschritte und nachvollziehbare Übergänge zwischen den Wiederaufnahmephasen zählen. Die Wiederanlaufsteuerung soll so gestaltet sein, dass sie nicht auf eine vollständige Wiederaufnahme in einem Schritt abzielt, sondern auf eine kontrollierte, priorisierte und belastbare Wiederaufnahme des wesentlichen Dienstes.

Exkurs: Notfallreaktionsverfahren

Im Zusammenhang mit der Wiederanlaufsteuerung ist zu berücksichtigen, dass auch Notfallreaktionsverfahren für die Phase der Wiederaufnahme relevant sein können. Obwohl diese Verfahren primär der akuten Bewältigung zuzuordnen sind, bilden sie eine wesentliche Voraussetzung für einen geordneten Übergang in die Wiederaufnahme. Kritische Einrichtungen sollen daher Notfallreaktionsverfahren, Mehrkanalwarnsysteme mit Geo-Targeting-Fähigkeiten, klare Befehlsketten einschließlich einer verantwortlichen Ansprechperson für Öffentlichkeitsarbeit sowie gefahrenspezifische Standardarbeitsanweisungen (SOPs) sicherstellen, die auf standortspezifische Risiken zugeschnitten sind. Kritische Einrichtungen sollen Notfallausrüstung vorhalten. Zudem sollen Notfallreaktionsteams benannt und geschult werden. Außerdem soll sichergestellt werden, dass Evakuierungsverfahren vorbereitet und die entsprechenden Unterlagen zugänglich sind. Diese Verfahren sollen regelmäßig geübt werden. Die Abstimmung dieser Verfahren mit der Wiederanlaufsteuerung soll gewährleisten, dass der Übergang von der akuten Reaktion in die strukturierte Wiederaufnahme nahtlos erfolgen kann.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖNORM EN ISO 22301	Sicherheit und Resilienz – Business Continuity Management System – Anforderungen (Kap. 8.2; Kap. 8.3; Kap. 8.4; Kap. 8.5; Kap. 9.1; Kap. 9.3; Kap. 10)
ÖNORM EN ISO 22361	Sicherheit und Resilienz – Krisenmanagement – Leitlinien (Kap. 5.2; Kap. 5.3.4; Kap. 6; Kap. 7)
ÖNORM D 4902-3	Risikomanagement für Organisationen und Systeme – Leitfaden – Teil 3: Notfall-, Krisen- und Kontinuitäts-management – Anleitung zur Umsetzung der ISO 31000

Stand: 01. Juni 2026

Tipps

Mindestleistungen sollen so konkret wie möglich beschrieben werden. Allgemeine Formulierungen wie „Betrieb aufrechterhalten" oder „rasch wiederaufnehmen bzw. wiederherstellen" sind für die praktische Steuerung nur eingeschränkt geeignet.
Es soll vorab festgelegt werden, welche Leistungen in welcher Reihenfolge fortgesetzt oder wiederaufgenommen werden sollen und welche Ressourcen dafür jeweils zwingend erforderlich sind.
Wiederanlaufentscheidungen sollen nicht ausschließlich technisch gedacht werden. Maßgeblich soll sein, welche Funktionen für den wesentlichen Dienst tatsächlich zuerst benötigt werden und welche Abhängigkeiten dabei zu berücksichtigen sind.
Wo automatisierte oder digital gestützte Systeme besonders kritisch sind, sollen auch manuelle oder vereinfachte Ersatzbetriebsweisen mitgedacht werden, damit die Fortsetzung kritischer Leistungen nicht ausschließlich von der vollständigen Wiederherstellung abhängt.

3 Business Continuity Management sowie Not- und Ersatzverfahren

Kritische Einrichtungen sollen sicherstellen, dass für die Fortsetzung oder rasche Wiederaufnahme des wesentlichen Dienstes ein belastbarer Rahmen des Business Continuity Managements vorgesehen ist. Dieser soll die Grundlage dafür bilden, kritische Funktionen, erforderliche Mindestleistungen, Wiederaufnahmeprioritäten, Notbetriebsoptionen und Ersatzverfahren systematisch festzulegen und im Störungsfall geordnet anzuwenden. Ziel ist es, auch bei erheblichen Beeinträchtigungen handlungsfähig zu bleiben, den wesentlichen Dienst in priorisierter Form fortzuführen oder ihn in vertretbarer Zeit in einen belastbaren Betriebszustand zurückzuführen.

Business Continuity Management soll dabei nicht als isoliertes Dokumentationssystem, sondern als umsetzbares Steuerungsmodell für Kontinuität und Wiederaufnahme verstanden werden. Kritische Einrichtungen sollen daher vorab festlegen, welche Funktionen und Leistungen im Störungsfall weiterzuführen sind, welche Not- und Ersatzverfahren dafür zur Verfügung stehen und unter welchen Voraussetzungen diese aktiviert, angepasst oder deaktiviert werden sollen. Dies soll insbesondere auch den Fall abdecken, dass reguläre Betriebsabläufe nicht mehr funktionieren oder automatisierte Systeme und zentrale Unterstützungsfunktionen nur eingeschränkt oder nicht mehr verfügbar sind.

Kritische Einrichtungen sollen – unbeschadet der NIS-2-Richtlinie – umfassende Business Continuity Pläne (BCP) auf Grundlage von Business Impact Analysen entwickeln und aufrechterhalten, die kritische Funktionen identifizieren, Wiederaufnahmeprioritäten festlegen sowie Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO) definieren. BCP sollen klare Aktivierungskriterien, Ressourcenzuweisung, Rollen und Koordinierungsmechanismen für die Phasen Reaktion, Wiederherstellung, Wiederaufnahme und Rückkehr zum Normalbetrieb festlegen. Daraus folgt, dass Business Continuity Management die Kontinuitäts- und Wiederherstellungsfähigkeit nicht nur abstrakt beschreibt, sondern in konkrete, aktivierbare Verfahren überführt.

Not- und Ersatzverfahren sollen insbesondere dort vorgesehen werden, wo der wesentliche Dienst oder besonders kritische Teilleistungen nicht bis zur vollständigen Wiederaufnahme regulärer Systeme ausgesetzt werden können. Kritische Einrichtungen sollen daher festlegen, welche Prozesse in vereinfachter, manueller, alternativer oder temporär reduzierter Form fortgeführt werden sollen, welche Ressourcen dafür erforderlich sind und wie lange diese Verfahren tragfähig angewendet werden können. Not- und Ersatzverfahren sollen damit nicht als bloße Überbrückung ohne Steuerungslogik verstanden werden, sondern als bewusst vorbereitete Betriebsoptionen zur Aufrechterhaltung kritischer Leistungen.

Business Continuity Management sowie Not- und Ersatzverfahren sollen darüber hinaus die Übergänge zwischen Reaktion, Wiederherstellung, Wiederaufnahme und Rückkehr in den Normalbetrieb berücksichtigen. Dazu sollen Krisenmanagementverfahren Incident-Command-Strukturen (ICS) mit klar definierten Entscheidungsbefugnissen und dokumentierten Aktionsplänen umfassen. Kritische Einrichtungen sollen die Etablierung von Krisenteams mit vordefinierten Rollen, Eskalationsprotokollen und Kommunikationskanälen (primär und alternativ) in Betracht ziehen, um eine rasche und koordinierte Reaktion auf relevante Ereignisse sicherzustellen. Aktivierungskriterien, Freigaben, Rollen, Zuständigkeiten und Eskalationsmechanismen sollen so festgelegt werden, dass im Ereignisfall keine Unklarheit darüber besteht, wann der Übergang von einer Phase in die nächste erfolgen soll.

Kommunikation soll auch in der Phase der Wiederaufnahme als eigenständige Führungs- und Steuerungsaufgabe verstanden und in das Business Continuity Management eingebettet werden. Kritische Einrichtungen sollen daher vorsehen, wie

interne und externe Anspruchsgruppen über Einschränkungen, Prioritäten, Zeitpläne, Freigaben und Wiederanlaufschritte informiert werden. Dafür sollen Strukturen und Prozesse für Krisenkommunikation geschaffen werden, um einen zeitnahen und korrekten Informationsfluss an interne und externe Stakeholder (einschließlich Kunden und Öffentlichkeit) sicherzustellen. Kritische Einrichtungen sollen vorab freigegebene Kommunikationsvorlagen, Routinen zur Stakeholder-Benachrichtigung und Multi-Channel-Kommunikationsfähigkeiten, einschließlich redundanter Systeme, vorhalten. Kommunikationsregelungen sollen sicherstellen, dass Informationen zeitgerecht, konsistent und adressatengerecht in belastbaren Freigabeprozessen weitergegeben werden.

Soweit für die Fortsetzung des wesentlichen Dienstes alternative Betriebsformen, Ausweichlösungen oder ausgelagerte Wiederherstellungsoptionen erforderlich sind, sollen diese in das Business Continuity Management sowie in die Not- und Ersatzverfahren integriert werden. Dabei soll sichergestellt sein, dass solche Lösungen nicht nur technisch vorgesehen, sondern auch organisatorisch, personell und prozessual nutzbar sind. Die konkrete Ausgestaltung von Ausweichstandorten, Backups und sonstigen alternativen Lösungen erfolgt im Rahmen der Ressourcen- und Redundanzenplanung.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖNORM EN ISO 22301	Sicherheit und Resilienz – Business Continuity Management System – Anforderungen
ÖNORM EN ISO 22313	Sicherheit und Resilienz – Business Continuity Management Systems – Anleitung zur Verwendung von ISO 22301
ÖNORM EN ISO 22361	Sicherheit und Resilienz – Krisenmanagement – Leitlinien
ÖNORM D 4902-3	Risikomanagement für Organisationen und Systeme – Leitfaden – Teil 3: Notfall-, Krisen- und Kontinuitätsmanagement – Anleitung zur Umsetzung der ISO 31000
ISO 22316	Security and resilience – Organizational resilience – Principles and attributes
ISO/TS 22317	Security and resilience – Business continuity management systems – Guidelines for business impact analysis
ISO/TS 22331	Security and resilience – Business continuity management systems – Guidelines for business continuity strategy
ISO/TS 22332	Security and resilience – Business continuity management systems – Guidelines for developing business continuity plans and procedures

Stand: 01. Juni 2026

Tipps

Business Continuity Management soll so ausgestaltet werden, dass es im Ereignisfall tatsächlich als Steuerungsinstrument genutzt werden kann. Zu abstrakte oder stark generische Pläne sind für die operative Anwendung häufig nur eingeschränkt geeignet.
Not- und Ersatzverfahren sollen nicht nur beschrieben, sondern in ihrer praktischen Anwendbarkeit geprüft werden. Dabei soll insbesondere berücksichtigt werden, ob Personal, Ressourcen, Zugriffe, Kommunikationswege und Freigaben im Störungsfall tatsächlich verfügbar sind.
Im Rahmen der Business Impact Analyse soll der Fokus nicht nur auf Prozessen, sondern auf der tatsächlichen Erbringung der wesentlichen Dienste liegen. Es soll daher zuerst geklärt werden, welche Leistungen oder Teilleistungen tatsächlich kritisch sind – danach erst, welche Prozesse, Systeme, Personen, Standorte und Ressourcen diese Leistungen ermöglichen.
RTO, RPO und maximale tolerierbare Ausfallszeit sollen nicht isoliert oder rein technisch festgelegt werden. Sie sollen aus tatsächlichen Schadensverläufen und der betrieblichen Tragfähigkeit abgeleitet werden. Ein formal definierter Zielwert ist nur dann belastbar, wenn nachvollziehbar ist, warum genau dieser Zeitraum für die jeweilige Funktion noch vertretbar ist.
Kommunikation in der Wiederaufnahmephase soll nicht zu spät beginnen. Es soll frühzeitig festgelegt werden, welche Anspruchsgruppen wann, in welcher Tiefe und über welche Kanäle informiert werden sollen. Unklare Sprecherrollen oder parallele Kommunikationswege erhöhen das Risiko widersprüchlicher Aussagen und erschweren die Koordination mit Behörden und externen Partnern.

4 Ressourcen, Redundanzen und alternative Lösungen

Kritische Einrichtungen sollen sicherstellen, dass für die Fortsetzung oder rasche Wiederaufnahme der wesentlichen Dienste kritische Ressourcen, Redundanzen und alternative Lösungen systematisch berücksichtigt werden. Dazu sollen insbesondere Personal, IT- und OT-Systeme, Gebäude, Standorte, Kommunikationsmittel, Energieversorgung, Medien, Transport, Rohstoffe, Hilfsstoffe, Ersatzteile sowie externe Dienstleistungen zählen. Ziel ist es, auch bei Ausfall oder eingeschränkter Verfügbarkeit primärer Systeme, Standorte oder Ressourcen handlungsfähig zu bleiben und den wesentlichen Dienst in einem belastbaren Umfang fortzuführen oder wiederaufzunehmen.

Kritische Einrichtungen sollen daher vorab festlegen, welche Ressourcen und Unterstützungsleistungen für die Aufrechterhaltung von Mindestleistungen und für die Wiederaufnahme kritischer Funktionen zwingend erforderlich sind. Dazu sollen Abhängigkeiten identifiziert, nach ihrer Bedeutung für den wesentlichen Dienst bewertet und mit geeigneten Maßnahmen abgesichert werden. Dies soll insbesondere dort gelten, wo der Ausfall einzelner Ressourcen oder Infrastrukturen die Fortsetzung

des wesentlichen Dienstes erheblich erschwert, verzögert oder unmöglich macht. Die Ressourcenbetrachtung soll sich dabei nicht auf einzelne Komponenten beschränken, sondern die gesamte Funktionsfähigkeit des Systems in den Blick nehmen.

Hinsichtlich der Sicherstellung der Kontinuität des Betriebs sollen Redundanzmaßnahmen in Betracht gezogen werden, die gewährleisten, dass wesentliche Dienste weiter bereitgestellt werden, wenn Primärsysteme ausfallen. Daraus folgt, dass Redundanzen und alternative Lösungen nicht nur technisch, sondern auch organisatorisch und personell mitgedacht werden sollen.

Alternative Standorte stellen ein wesentliches Element der Wiederherstellungsfähigkeit dar und sollen daher in Betracht gezogen werden. Diese können entweder als „Hot Sites" (voll ausgestattet für die sofortige Nutzung), „Warm Sites" (teilweise ausgestattet) oder „Cold Sites" (erfordern eine Einrichtung nach der Störung) gestaltet sein. Backup-Standorte sollen ausreichend weit von den primären Einrichtungen entfernt sein und zugleich erreichbar bleiben. Wo möglich, sollen auch mobile Einrichtungen (z.B. Leitstellen/Command Centres) in Betracht gezogen werden. Backups sollen an physisch getrennten oder logisch isolierten Standorten gespeichert werden. Daraus folgt, dass alternative Lösungen nicht nur nominell vorhanden sein sollen, sondern auch hinsichtlich Distanz, Erreichbarkeit, Nutzbarkeit und Schutz gegen gemeinsame Ausfallursachen belastbar geplant werden sollen.

Ein grundlegendes Element ist die mehrstufige Redundanz. Die EU-Guidelines betonen, dass es möglich sein soll, Dienste über grenzüberschreitende, nationale, regionale und lokale Ebenen hinweg mit wirksamer Interoperabilität zu erbringen. Für kritische Einrichtungen folgt daraus, dass Redundanz nicht nur als Doppelung einzelner Komponenten verstanden werden soll, sondern als strukturelle Fähigkeit, Funktionen auch bei Ausfall bestimmter Ebenen oder Knotenpunkte geordnet fortzuführen.

Ein besonderer Schwerpunkt soll auf Personal und organisatorischer Einsatzfähigkeit liegen. Kritische Einrichtungen sollen im Rahmen ihrer Ressourcenplanung auch personelle Engpässe, Ausfälle von Schlüsselrollen und länger andauernde Belastungen berücksichtigen. In diesem Zusammenhang soll die Personalplanung Anforderungen an Spitzenlast- und Zusatzkapazitäten durch Vorhalten eines Bereitschaftspools, Schulungsprogramme und vorab vereinbarte gegenseitige Unterstützungsabkommen mit Partnerorganisationen adressieren. Ebenso sollen Kompetenzrahmen und Nachfolgeplanung entwickelt werden, um eine ausreichende personelle Tiefe in kritischen Rollen sicherzustellen und die Betriebsfähigkeit bei länger andauernden Störungen oder Personalknappheit aufrechtzuerhalten. Personelle Redundanz und alternative Einsatzfähigkeit sollen damit integraler Bestandteil der Kontinuitäts- und Wiederaufnahmeplanung sein.

Ressourcen, Redundanzen und alternative Lösungen sollen darüber hinaus die Verfügbarkeit kritischer technischer und logistischer Unterstützungsleistungen umfassen. Dazu sollen insbesondere Backups, Kommunikationsmittel, Energieversorgung, Transportmöglichkeiten, externe Dienstleister, Ersatzteile, Rohstoffe und Hilfs-

stoffe zählen. Je nach Sektor und Betriebsmodell sollen auch mobile Lösungen, Ausweicharbeitsplätze, alternative Netz- oder Datenanbindungen sowie physisch oder logisch getrennte Systemumgebungen berücksichtigt werden. Die Einrichtung soll vorab festlegen, welche dieser Lösungen für Mindestleistungen oder priorisierte Wiederanläufe zwingend erforderlich sind und unter welchen Voraussetzungen sie aktiviert werden sollen.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖNORM EN ISO 22301	Sicherheit und Resilienz – Business Continuity Management System – Anforderungen (Kap. 8.2; Kap. 8.3; Kap. 8.4; Kap. 8.5; Kap. 9.1; Kap. 9.3; Kap. 10)
ÖNORM EN ISO 22313	Sicherheit und Resilienz – Business Continuity Management Systems – Anleitung zur Verwendung von ISO 22301
ÖNORM EN ISO 22361	Sicherheit und Resilienz – Krisenmanagement – Leitlinien (Kap. 5.2; Kap. 5.3.4; Kap. 6; Kap. 7; Kap. 9)
ÖNORM D 4902-3	Risikomanagement für Organisationen und Systeme – Leitfaden – Teil 3: Notfall-, Krisen- und Kontinuitäts-management – Anleitung zur Umsetzung der ISO 31000
ISO 22316	Security and resilience – Organizational resilience – Principles and attributes
ISO/TS 22317	Security and resilience – Business continuity management systems – Guidelines for business impact analysis
ISO/TS 22318	Security and resilience – Business continuity management systems – Guidelines for supply chain continuity management
ISO/TS 22330	Security and resilience – Business continuity management systems – Guidelines for people aspects of business continuity
ISO/TS 22331	Security and resilience – Business continuity management systems – Guidelines for business continuity strategy
ISO/TS 22332	Security and resilience – Business continuity management systems – Guidelines for developing business continuity plans and procedures
ISO 28000	Security and resilience – Security management systems – Requirements

Stand: 01. Juni 2026

Tipps

Redundanzen sollen nicht nur technisch vorhanden, sondern auch praktisch nutzbar sein. Es soll daher vorab geklärt werden, ob alternative Standorte, Systeme oder Ressourcen im Ereignisfall tatsächlich erreichbar, aktivierbar und personell bedienbar sind.
Bei Ausweichstandorten und Backup-Lösungen sollen nicht nur die technische Verfügbarkeit, sondern auch Zugriffsrechte, Kommunikationswege, Freigabelogiken, Transportfähigkeit und personelle Besetzung berücksichtigt werden.
Personelle Redundanz soll frühzeitig mitgedacht werden. Kritische Rollen sollen nicht nur besetzt, sondern auch vertreten, geschult und im Ereignisfall durchhaltbar organisiert sein.
Es soll geprüft werden, ob alternative Lösungen gegen gemeinsame Ausfallursachen geschützt sind. Räumlich nahe Backups oder personell ident besetzte Ausweichstrukturen schaffen häufig nur scheinbare Resilienz.

5 Lieferketten, Ersatzbeschaffung und Versorgungssicherheit

Kritische Einrichtungen sollen sicherstellen, dass für die Fortsetzung oder rasche Wiederherstellung des wesentlichen Dienstes auch lieferkettenbezogene Abhängigkeiten, Ersatzbeschaffung und Versorgungssicherheit systematisch berücksichtigt werden. Dazu sollen insbesondere kritische Lieferanten, Bezugsquellen, logistische Schnittstellen, externe Unterstützungsleistungen, Sicherheitsbestände sowie alternative Liefer- und Versorgungspfade zählen. Ziel ist es, den wesentlichen Dienst auch dann fortführen oder wiederaufnehmen zu können, wenn Sicherheitsvorfälle zentrale Lieferketten, Dienstleister oder Versorgungsbeziehungen beeinträchtigen.

Kritische Einrichtungen sollen daher die für die wesentlichen Dienste relevanten Lieferketten und Unterstützungsleistungen identifizieren, kritische Abhängigkeiten bewerten und die Auswirkungen eines Ausfalls wesentlicher Lieferanten, Ressourcen oder Transportwege in ihre Planung einbeziehen. Dabei soll nicht nur die unmittelbare Beschaffung einzelner Güter betrachtet werden, sondern die gesamte Fähigkeit, notwendige Materialien, Komponenten, Dienstleistungen und Unterstützungsleistungen in der erforderlichen Zeit, Qualität und Menge verfügbar zu machen. Dies soll insbesondere dort gelten, wo der Ausfall einzelner Lieferbeziehungen die Wiederaufnahme wesentlicher Leistungen verzögern oder verhindern kann.

Lieferkettenresilienz ist ein wesentlicher Bestandteil der Wiederaufnahmefähigkeit. Kritische Einrichtungen sollen daher die Lieferketten im Zusammenhang mit der Erbringung ihrer wesentlichen Dienste erfassen, langfristige Strategien zur Lieferkettenresilienz entwickeln sowie einen Lieferketten-Notfallplan erstellen, regelmäßig überprüfen und aktualisieren. Ebenso sollen sie alternative Lieferketten identifizieren, falls erhebliche Störungen ihre Schlüssellieferanten betreffen. Daraus folgt, dass Liefer-

kettenresilienz nicht nur als Beschaffungsthema, sondern als integraler Bestandteil der Kontinuitäts- und Wiederherstellungsfähigkeit verstanden werden soll.

Ersatzbeschaffung und alternative Bezugswege sollen insbesondere dort vorbereitet werden, wo für die Wiederaufnahme des wesentlichen Dienstes bestimmte Rohstoffe, Hilfsstoffe, Chemikalien, Ersatzteile, Energie- oder Medienleistungen oder technische Dienstleistungen unverzichtbar sind. Kritische Einrichtungen sollen daher prüfen, welche Materialien, Komponenten oder Leistungen nicht kurzfristig substituierbar sind, welche Abhängigkeiten zu einzelnen Herstellern, Lieferanten oder Regionen bestehen und welche Alternativen im Ereignisfall tatsächlich verfügbar und nutzbar sind. Dies soll auch vertragliche, logistische und qualitätsbezogene Voraussetzungen umfassen.

Versorgungssicherheit soll darüber hinaus auch durch angemessene Bevorratung unterstützt werden. Kritische Einrichtungen sollen strategische Bevorratung in Betracht ziehen, einschließlich Pufferbeständen, Mechanismen für schnelle Nachlieferung und außerhalb des Standorts gelagerten Beständen, die vor verbreiteten Bedrohungen geschützt sind, damit der wesentliche Dienst bei einem Ausfall der Lieferkette nicht unterbrochen wird. Sicherheitsbestände sollen damit nicht isoliert als Lagerfrage, sondern als gezielte Resilienzmaßnahme zur Überbrückung von Lieferunterbrechungen und zur Stabilisierung prioritärer Leistungen verstanden werden.

Soweit dies aufgrund des Risikoprofils und des wesentlichen Dienstes erforderlich ist, sollen auch formalisierte Unterstützungsvereinbarungen mit Dritten vorgesehen werden. In Betracht gezogen werden kann der Abschluss formeller Verträge mit anderen Einrichtungen im selben Sektor über die gemeinsame Nutzung von Ressourcen, Ausrüstung oder Personal für den Fall eines umfangreichen Wiederherstellungsaufwands. Solche Vereinbarungen sollen insbesondere dort geprüft werden, wo eine kritische Einrichtung im Ereignisfall auf sektorinterne Kooperation, gegenseitige Hilfe oder rasch verfügbare Ersatzressourcen angewiesen sein kann.

Lieferketten, Ersatzbeschaffung und Versorgungssicherheit sollen nicht isoliert von den in Kapitel 2 dieses Leitfadens festgelegten Mindestleistungen und Wiederherstellungsprioritäten betrachtet werden. Vielmehr soll klar sein, welche Lieferungen, Ressourcen und Unterstützungsleistungen für welche prioritären Funktionen in welcher Reihenfolge benötigt werden. Ersatzbeschaffung soll daher nicht nur allgemein vorbereitet, sondern an den tatsächlich priorisierten Wiederherstellungsbedarfen ausgerichtet werden.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖNORM EN ISO 22301	Sicherheit und Resilienz – Business Continuity Management System – Anforderungen (Kap. 8.4; Kap. 8.5; Kap. 9.1; Kap. 9.2; Kap. 9.3; Kap. 10)
ÖNORM EN ISO 22313	Sicherheit und Resilienz – Business Continuity Management Systems – Anleitung zur Verwendung von ISO 22301
ÖNORM EN ISO 22361	Sicherheit und Resilienz – Krisenmanagement – Leitlinien (Kap. 6; Kap. 8; Kap. 9)
ISO 22398	Societal security – Guidelines for exercises
ÖNORM D 4902-3	Risikomanagement für Organisationen und Systeme – Leitfaden – Teil 3: Notfall-, Krisen- und Kontinuitätsmanagement – Anleitung zur Umsetzung der ISO 31000

Stand: 01. Juni 2026

Tipps

Kritische Lieferketten sollen nicht nur auf Ebene direkter Lieferanten betrachtet werden. Es soll auch geprüft werden, ob Vorprodukte, Logistik, externe Dienstleistungen oder regionale Konzentrationen zu verdeckten Abhängigkeiten führen.
Es soll vorab festgelegt werden, welche Materialien, Komponenten und Leistungen für welche prioritären Funktionen zwingend benötigt werden und in welcher Reihenfolge sie für Fortsetzung oder Wiederaufnahme verfügbar sein müssen.
Sicherheitsbestände sollen nicht pauschal, sondern risikobasiert festgelegt werden. Dabei sollen insbesondere Wiederbeschaffungszeiten, Substitutionsmöglichkeiten, Verbrauchsdynamik und Schutz gegen gemeinsame Ausfallursachen berücksichtigt werden.
Alternative Lieferanten oder Bezugswege sollen nicht nur theoretisch benannt, sondern soweit möglich vorab qualifiziert, vertraglich vorbereitet und praktisch auf ihre Nutzbarkeit im Ereignisfall geprüft werden.

6 Abschließende Vorgaben

Für die Umsetzung des Leitfadens Z 4 wird nochmals darauf hingewiesen, dass sämtliche Anforderungen auf den wesentlichen Dienst der kritischen Einrichtung bezogen sind. Die Resilienzmaßnahmen gemäß § 15 RKEG dienen nicht dem allgemeinen Schutz der Einrichtung als Unternehmen, sondern der Aufrechterhaltung der Fähigkeit, den wesentlichen Dienst zu erbringen. Ebenso sind die Grundsätze der Geeignetheit und Verhältnismäßigkeit, der Konformitätsvermutung einschließlich der Begründung bei Abweichungen, des Verhältnisses zu Normen und Richtlinien sowie der Stufenlogik der behördlichen Prüfung, wie in Leitfaden Z 0 dargelegt, zu beachten. Dem risikobasierten Ansatz folgend liegt die konkrete Ausgestaltung bei der kritischen Einrichtung selbst.

Die Kontinuitäts- und Wiederherstellungsfunktion der vorgesehenen Maßnahmen soll dauerhaft aufrechterhalten werden. Soweit hierfür Wartung, Übung, Testung, Überprüfung, Aktualisierung oder sonstige wiederkehrende Maßnahmen erforderlich sind, sollen diese verbindlich vorgesehen und nachvollziehbar dokumentiert werden. Business-Continuity-Pläne sollen getestet, überprüft und in geplanten Abständen sowie nach jedem Sicherheitsvorfall oder jeder wesentlichen Änderung des Betriebs aktualisiert werden. Gewonnene Erkenntnisse aus Übungen, Vorfällen und Testungen sollen systematisch ausgewertet und in Verbesserungsmaßnahmen überführt werden.

Dazu sollen Untersuchungen nach einem Sicherheitsvorfall strukturierte Methoden wie die Ursachenanalyse (Root Cause Analysis) verwenden, um systemische Ursachen statt unmittelbarer Symptome zu identifizieren. Ebenso sollen nach allen Übungen und tatsächlichen Vorfällen After Action Reviews (AAR) durchgeführt werden, um gewonnene Erkenntnisse zu erfassen. Die Ergebnisse sollen systematisch dokumentiert und in aktualisierte Verfahren, Schulungsprogramme und einrichtungsinterne Risikoanalysen integriert werden, um Wiederholungen zu verhindern und die organisatorische Resilienz zu stärken.

Es ist die Aufgabe der kritischen Einrichtung, im Resilienzplan nachvollziehbar darzulegen, wie sie den Anforderungen im Einzelnen entspricht: welche kritischen Funktionen, Mindestleistungen, Abhängigkeiten und Wiederherstellungsanforderungen berücksichtigt wurden; welche Szenarien der Planung zugrunde liegen; welche Prioritäten daraus abgeleitet wurden und mit welchem abgestimmten Maßnahmenbündel aus technischen, organisatorischen, personellen, lieferkettenbezogenen und kommunikativen Komponenten die fortgesetzte Erbringung oder Wiederaufnahme des wesentlichen Dienstes erreicht werden soll.

Z 5: Personelle Sicherheits-vorkehrungen

1 Allgemeine Grundlagen

Kritische Einrichtungen haben geeignete und verhältnismäßige Resilienzmaßnahmen zu treffen, um angemessene personelle Sicherheitsvorkehrungen zu gewährleisten. Personal – eigenes wie externes – trägt in jeder Phase zur Resilienz bei: von der Prävention und Erkennung von Bedrohungen über die Reaktion auf Vorfälle bis hin zur Sicherstellung der Kontinuität des wesentlichen Dienstes. Zugleich gehen von Personal auch spezifische Risiken aus, die gezielt zu adressieren sind.

Personalbezogene Bedrohungen sind systematisch zu bewerten und zu behandeln. Dies umfasst sowohl vorsätzliche Handlungen wie Spionage, Manipulation oder gezielte Schädigung als auch nicht-vorsätzliche Gefährdungen wie unzureichende Qualifikation, Überlastung oder mangelndes Sicherheitsbewusstsein.

Der vorliegende Leitfaden Z 5 behandelt die strukturelle personelle Absicherung entlang folgender Schwerpunkte: die Identifikation kritischer Funktionen und deren Dokumentation, die Steuerung von Zugangsberechtigungen, die Durchführung von Zuverlässigkeitsüberprüfungen sowie die Festlegung von Ausbildungs- und Qualifikationsanforderungen. Die physische und technische Umsetzung der Zutrittssteuerung – also zonale Architektur, Zutrittskontrollsysteme und physische Barrieren – wird im Leitfaden Z 2 geregelt. Die konkrete Umsetzung durch Schulungsformate, Informationsmaterialien und Übungen ist Gegenstand des Leitfadens Z 6.

Darüber hinaus sollen kritische Einrichtungen die Integration von Geschlechtergleichstellung in die Resilienzplanung und -maßnahmen berücksichtigen, indem sie ein ausgewogenes Geschlechterverhältnis in ihrer Organisationsstruktur (z.B. in Führungs- und Krisenteams) sicherstellen und prüfen, wie sich Störungen unterschiedlich auf Frauen und Männer auswirken.

Vernetzend mit der NIS-2-Richtlinie ist festzuhalten, dass personelle Sicherheitsmaßnahmen gemäß Art. 21 Abs. 2 Buchstabe i NIS-2-RL integriert und nicht parallel aufgebaut werden sollen (siehe Leitfaden Z 5, Kapitel 4).

2 Identifikation und Dokumentation kritischer Funktionen

Kritische Einrichtungen sollen systematisch ermitteln, welche Funktionen und Rollen unmittelbar oder mittelbar für die Erbringung der wesentlichen Dienste erforderlich sind. Das Ergebnis dieser Ermittlung bildet die Grundlage für alle weiteren personellen Sicherheitsvorkehrungen – von der Zugangssteuerung über die Zuverlässigkeitsüberprüfung bis hin zu den Qualifikationsanforderungen.

Kritische Einrichtungen sollen daher Kategorien von kritische Funktionen ausübendem Personal identifizieren und entsprechende Listen erstellen, unter Einbeziehung des Personals externer Dienstleister (Auftragnehmer und Subauftragnehmer). Externes Personal ist dabei besonders zu berücksichtigen, da es häufig Zugang zu kritischer

Infrastruktur oder sensiblen Systemen hat, ohne den internen Kontrollmechanismen unmittelbar zu unterliegen. Einzubeziehen sind insbesondere Sicherheitsdienstleister, IT-Dienstleister, Wartungs- und Instandhaltungspersonal, Reinigungskräfte mit Zugang zu gesicherten Bereichen sowie Beratungsunternehmen mit Einblick in sicherheitsrelevante Planungen.

Bei der Erstellung dieser Listen sollen die Besonderheiten der erbrachten wesentlichen Dienste berücksichtigt und diese mit dem beteiligten Personal verknüpft werden. So wird transparent, welche Personen für welchen wesentlichen Dienst unverzichtbar sind und wo gezielter Handlungsbedarf bei Absicherung, Qualifizierung und Überprüfung besteht. Kritische Einrichtungen sollen eine klare, umfassende und aktuelle Dokumentation dieser Personalkategorien führen – nicht als einmalige Bestandsaufnahme, sondern als laufend gepflegtes Instrument, das Änderungen in Organisationsstruktur, Dienstleistungsverhältnissen oder Leistungsumfang zeitnah abbildet.

Auf Grundlage der identifizierten Kategorien soll festgelegt werden, welche Funktionen als sicherheitsempfindlich gelten. Kritische Einrichtungen sollen den Geltungsbereich und die Policy für Zuverlässigkeitsüberprüfungen definieren und direkten Zugang oder Fernzugang zuche Rollen als sicherheitsempfindlich gelten, welche Rollen einen direkten Zugang zu Liegenschaften, Informationen, Kontrollsystemen oder kritischen Prozessen haben. Die Einstufung als sicherheitsempfindlich zieht Konsequenzen für die Zugangsberechtigungen (siehe Leitfaden Z 5, Kapitel 3), die Verpflichtung zur Zuverlässigkeitsüberprüfung (siehe Leitfaden Z 5, Kapitel 4) und die erforderlichen Qualifikationsanforderungen (siehe Leitfaden Z 5, Kapitel 5) nach sich.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ISO/TS 22330	Security and resilience – Business continuity management systems – Guidelines for people aspects of business continuity (Kap. 5.4.; Kap. 6.3.; Kap. 6.5)
ÖVE/ÖNORM EN ISO/IEC 27002	Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Informationssicherheitsmaßnahmen (Kap. 6.1; Kap. 6.2)
ÖNORM EN 17483-1	Private Sicherheitsdienstleistungen – Schutz kritischer Infrastrukturen – Teil 1: Allgemeine Anforderungen (Kap. 6.1.3; Kap. 6.1.4)

Stand: 01. Juni 2026

Tipps

Kritischer Funktionen soll von den wesentlichen Diensten und nicht von der Organisationsstruktur ausgehend gedacht und identifiziert werden. Es soll zuerst geklärt werden, welche Leistungen kritisch sind, dann, welche Funktionen diese Leistungen ermöglichen, und erst dann, welche Personen diese Funktionen ausüben.
Bei externen Dienstleistern soll nicht nur die Firma als Vertragspartner erfasst werden, sondern auch die tatsächlich eingesetzten Personen, deren Rollen und deren Zugangsniveau. Ein reiner Vertragsverweis reicht für die Dokumentation kritischer Funktionen nicht aus.
Die Dokumentation soll so aufgebaut sein, dass bei einem Personalwechsel – intern wie extern – sofort erkennbar ist, welche Konsequenzen sich daraus für Zugangsberechtigungen, Überprüfungspflichten und Qualifikationsanforderungen ergeben.

3 Zugangsberechtigungen und personelle Zugriffskontrolle

Kritische Einrichtungen sollen sicherstellen, dass Zugangsberechtigungen zu Liegenschaften, kritischer Infrastruktur, sensiblen Informationen auf Grundlage klar definierter Kriterien vergeben, gesteuert und bei Bedarf unverzüglich entzogen werden. Während der Leitfaden Z 2 die technische und physische Umsetzung der Zutrittssteuerung – also zonale Architektur, Zutrittskontrollsysteme und physische Barrieren – behandelt, regelt das vorliegende Kapitel die personelle Steuerungslogik: Welche Personen bekommen auf Basis welcher Rollen und Berechtigungen welche Zugänge.

Kritische Einrichtungen sollen festlegen, wem und unter welchen Bedingungen Zugang zu Räumlichkeiten, kritischer Infrastruktur und sensiblen Informationen gewährt wird. Wirksame Prozesse zur Gewährung und sofortigen Entziehung des physischen und systemseitigen Zugangs sollen eingerichtet sein, und Zugangsrechte sollen strikt durchgesetzt werden. Die sofortige Entziehung ist dabei von besonderer Bedeutung: Bei Rollenwechsel, Aufgabenänderungen, organisatorischen Veränderungen, dem Ausscheiden von Personen oder bei Entzug der Sicherheitsfreigabe sollen Zugangsberechtigungen ohne Verzögerung angepasst oder entzogen werden.

Für die Vergabe von Zugangsberechtigungen soll das Prinzip der geringsten Privilegien gelten. Kritische Einrichtungen sollen Zugang ausschließlich nach dem Need-to-know-/Need-to-access-Prinzip gewähren, und nur der für die Erfüllung der jeweiligen Funktion erforderliche Zugang soll sichergestellt werden. Daraus folgt, dass kein Zugang pauschal, statusbezogen oder aus organisatorischer Gewohnheit vergeben werden soll, sondern ausschließlich auf Grundlage der tatsächlichen funktionalen Erfordernisse.

Für die wirksame Umsetzung dieses Prinzips sollen geeignete Steuerungsinstrumente eingesetzt werden. Umsetzungsstrategien wie rollenbasierte Zugriffskontrolle, starke Authentifizierung und Identitätsmanagement, Funktionstrennung, zeitbasierte

Einschränkungen und Just-in-Time-Zugang sollen gemeinsam mit einer regelmäßigen Auditierung und Überprüfung eingerichtet werden.

Rollenbasierte Zugriffskontrolle bedeutet, dass spezifische Rollen definiert und mit einem vordefinierten Umfang an Zugangsrechten versehen werden. Diese werden dann dem jeweiligen Personal zugewiesen. Starke Authentifizierung umfasst insbesondere Mehrfaktor-Authentifizierung und eindeutige Identifikationsmerkmale. Zeitbasierte Einschränkungen und Just-in-Time-Zugang bedeuten, dass Personal nur dann temporären Zugang erhält, wenn es diesen für bestimmte Aufgaben aktiv benötigt und der Zugang anschließend unverzüglich entzogen wird.

Die Zugangsberechtigungen sollen regelmäßig sowie anlassbezogen überprüft und auditiert werden. Dabei soll insbesondere geprüft werden, ob die vergebenen Berechtigungen noch der tatsächlichen Funktion der betreffenden Person entsprechen, ob inzwischen ausgeschiedene oder versetzte Personen noch über aktive Berechtigungen verfügen und ob die definierten Rollen und Zugangsniveaus noch mit dem aktuellen Schutzbedarf übereinstimmen.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖVE/ÖNORM EN ISO/IEC 27002	Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Informationssicherheitsmaßnahmen (Kap. 5.15; Kap. 5.18; Kap. 6.5; Kap. 8.2)
ÖNORM S 2415-1	Security Management System – Teil 1: Anforderungen an ein Security Management-System

Stand: 01. Juni 2026

Tipps

Die häufigste Schwachstelle in der Zugangssteuerung ist nicht das Fehlen eines Systems, sondern die mangelnde Aktualität: Berechtigungen werden vergeben, aber bei Rollenwechsel oder Ausscheiden nicht entzogen. Ein verbindlicher Prozess zur anlassbezogenen Überprüfung ist daher mindestens ebenso wichtig wie das technische System selbst.

Just-in-Time-Zugang kann insbesondere bei externen Dienstleistern und bei seltenen Wartungstätigkeiten ein wirksames Instrument sein, um das Zeitfenster möglicher Zugriffe auf das betrieblich Erforderliche zu begrenzen.

Die Funktionstrennung soll auch bei personellen Engpässen aufrechterhalten werden. Wo dies aufgrund der Organisationsgröße nicht durchgängig möglich ist, sollen kompensierende Maßnahmen wie Vier-Augen-Prinzip, Protokollierung oder nachgelagerte Kontrollen vorgesehen werden.

4 Zuverlässigkeitsüberprüfungen

Zuverlässigkeitsüberprüfungen sind ein wesentliches Instrument zur Absicherung kritischer Funktionen gegen Insider-Bedrohungen und zur Sicherstellung der Integrität des in sicherheitsempfindlichen Bereichen eingesetzten Personals. Sie ergänzen die im vorliegenden Leitfaden Z 5, Kapitel 3 dargestellte Zugangssteuerung um eine personenbezogene Überprüfungskomponente.

Kritische Einrichtungen sollen funktionierende interne Verfahren für die Beantragung von Zuverlässigkeitsüberprüfungen einrichten und die Kategorien von Personen festlegen, die solchen Überprüfungen zu unterziehen sind. Verfahren für den Umgang mit Personen, deren Sicherheitsfreigabe entzogen wird, sollen ebenfalls vorgesehen werden. Die Etablierung interner Verfahren ist dabei nicht nur als administrative Pflicht zu verstehen, sondern als Voraussetzung dafür, dass Zuverlässigkeitsüberprüfungen systematisch, nachvollziehbar und fristgerecht durchgeführt werden können.

Für die Festlegung des Geltungsbereichs sollen kritische Einrichtungen den Umfang und die Grundlagen zur Beurteilung der Zuverlässigkeit definieren und dabei festlegen, welche Rollen sicherheitsempfindlich sind, welche Rollen einen direkten oder Fernzugang zu Räumlichkeiten, Informationen, Kontrollsystemen, oder kritischen Prozesse haben und welche Arten von Überprüfungen für jede sicherheitsempfindliche Rolle durchzuführen sind – wie etwa Identitätsprüfung, Strafregisterauszüge, Beschäftigungs-, Ausbildungsnachweise und Zuverlässigkeitsüberprüfung. Die Grundlagen zur Beurteilung der Zuverlässigkeit ermöglichen damit eine differenzierte Steuerung: Nicht jede Rolle erfordert denselben Überprüfungsumfang, aber für jede sicherheitsempfindliche Rolle soll transparent und nachvollziehbar festgelegt sein, welche Überprüfungen vorgesehen sind, in welchen Intervallen diese stattzufinden haben, welche Anhaltspunkte eine erneute Überprüfung erforderlich machen (z.B. aufgrund konkreter Verdachtsmomente, oder wenn die Person eine andere sicherheitsempfindliche Funktion übernimmt).

Besonderes Augenmerk soll auf den Umgang mit dem Ergebnis der Überprüfung gelegt werden. Für Fälle, in denen eine Sicherheitsfreigabe nicht erteilt oder nachträglich entzogen wird, sollen klare Verfahren vorgesehen werden. Diese sollen insbesondere regeln, wie die betreffende Person über das Ergebnis informiert wird, welche Konsequenzen für Zugangsberechtigungen und Aufgabenzuweisungen gezogen werden, wie der Übergang organisiert wird und welche datenschutzrechtlichen Anforderungen dabei zu beachten sind.

Für die praktische Durchführung der Zuverlässigkeitsüberprüfung wird auf die aktuellen Leitfäden zu Sicherheits- und Zuverlässigkeitsüberprüfungen des Bundesministeriums für Inneres verwiesen, welche die Verfahrensabläufe, Datenanforderungen und Fristen im Detail beschreiben.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖVE/ÖNORM EN ISO/IEC 27002	Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Informationssicherheitsmaßnahmen (Kap. 6.1)
ÖNORM EN 17483-1	Private Sicherheitsdienstleistungen – Schutz kritischer Infrastrukturen – Teil 1: Allgemeine Anforderungen (Kap. 6.1.3)

Stand: 01. Juni 2026

Tipps

Ins rechte Licht gerückt führen Zuverlässigkeitsprüfungen dazu, dass Mitarbeitende sie nicht als Kontrolle, sondern als das wahrnehmen, was sie sind, nämlich eine Auszeichnung und ein Ausdruck von Integrität und Verantwortung.
Nicht jede sicherheitsempfindliche Rolle erfordert denselben Überprüfungsumfang. Eine abgestufte Regelung vermeidet sowohl Lücken als auch unverhältnismäßigen Aufwand.
Tritt der Entzug einer Sicherheitsfreigabe ein, zählt jede Stunde: Wer nicht vorab geregelt hat, wie eine betroffene Person aus sicherheitsempfindlichen Bereichen und Funktionen herausgelöst wird, regelt es unter Druck – mit allen Risiken.

5 Anforderungen an Ausbildung und Qualifikation

Die Festlegung angemessener Ausbildungs- und Qualifikationsanforderungen ist Bestandteil der Gewährleistung eines angemessenen personellen Sicherheitsmanagements, der Sensibilisierung des Personals und der Unterstützung der von der kritischen Einrichtung getroffenen Resilienzmaßnahmen.

Die einrichtungsinterne Risikoanalyse, die Art der von ihr erbrachten wesentlichen Dienste sowie die geplanten oder getroffenen Maßnahmen sollen Art und Umfang der für das Personal der jeweiligen Einrichtung erforderlichen Schulung bestimmen. Das Ziel ist, sicherzustellen, dass das Personal nicht nur allgemein sensibilisiert, sondern auch technisch und prozessual in der Lage ist, seine Aufgaben auf resiliente Weise auszuführen. Die Anforderungen an Schulung und Qualifikation beziehen sich unter anderem auf die einrichtungsinterne Risikoanalyse (z.B. für Management-/Risiko-Compliance-Personal), auf Business Continuity und Krisenmanagement (z.B. für Business Continuity Personal), auf physische Sicherheit (z.B. für Sicherheitspersonal und Personen mit Zugangsrechten), auf Vorfallsreaktion und -bewältigung (z.B. für operatives Personal und benannte Vorfallsreaktionskräfte), auf Zutrittskontrolle und Überprüfung (HR, Sicherheit und Führungskräfte kritischer Funktionen) sowie auf die allgemeine Sensibilisierung aller Mitarbeitenden.

Ziel dieser Anforderungen soll es sein, die Kompetenz des Personals zur Ausführung der in der einrichtungsinternen Risikoanalyse, dem Resilienzplan und den darin

eingebetteten Business Continuity Verfahren festgelegten Aufgaben sicherzustellen. Die Qualifikationen beziehen sich auf operative und technische, organisatorische und Management- oder sicherheits- und überprüfungsbezogene Aufgaben. Die erforderlichen Qualifikationen sollen in den internen Resilienz- und HR-Policys der kritischen Einrichtung definiert werden.

Die interne Verankerung in Resilienz- und HR-Policys stellt sicher, dass Qualifikationsanforderungen nicht als abstrakte Vorgaben bestehen, sondern operativ umgesetzt, überwacht und bei Bedarf angepasst werden. Sie bilden die Grundlage für gezielte Schulungsplanung, Kompetenzbewertung und Nachweisführung. Die konkrete Umsetzung durch Schulungsformate, Informationsmaterialien und Übungen ist Gegenstand des Leitfadens Z 6.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖNORM ISO 10015	Qualitätsmanagement – Leitfaden für Kompetenzmanagement und Personalentwicklung (Kap. 4.2; Kap. 4.3; Kap. 5)
ÖNORM EN ISO 22301	Sicherheit und Resilienz – Business Continuity Management System – Anforderungen (Kap. 7.2)
ÖNORM EN ISO 22361	Sicherheit und Resilienz – Krisenmanagement – Leitlinien (Kap. 9)
ISO/TS 22330	Security and resilience – Business continuity management systems – Guidelines for people aspects of business continuity (Kap. 5.4; Kap. 6.5)
ÖNORM EN 17483-1	Private Sicherheitsdienstleistungen – Schutz kritischer Infrastrukturen – Teil 1: Allgemeine Anforderungen (Kap. 6.3)
ÖNORM D 4902-3	Risikomanagement für Organisationen und Systeme – Leitfaden – Teil 3: Notfall-, Krisen- und Kontinuitätsmanagement

Stand: 01. Juni 2026

Tipps

Qualifikationsanforderungen sollen so konkret wie möglich formuliert werden. Allgemeine Formulierungen wie „Personal ist angemessen zu schulen" sind für die Nachweisführung und behördliche Überprüfung nicht ausreichend. Es soll für jede kritische Funktion klar sein, welche Kompetenzen erforderlich sind und wie deren Vorliegen nachgewiesen wird.

Die Differenzierung nach Funktionsbereichen soll nicht nur auf dem Papier bestehen. Sicherheitspersonal benötigt andere Kompetenzen als Personal für Krisenmanagement oder IT-Administration. Einheitliche Schulungsprogramme für alle können dazu führen, dass funktionsspezifische Kompetenzlücken unerkannt bleiben.

Bei externem Personal sollen die Qualifikationsanforderungen vertraglich verankert und deren Einhaltung regelmäßig überprüft werden. Der Nachweis der Qualifikation des eingesetzten Personals soll nicht ausschließlich dem Dienstleister überlassen, sondern von der kritischen Einrichtung aktiv eingefordert und dokumentiert werden.

6 Abschließende Vorgaben

Für die Umsetzung des Leitfadens Z 5 wird nochmals darauf hingewiesen, dass sämtliche Anforderungen auf den wesentlichen Dienst der kritischen Einrichtung bezogen sind. Die Resilienzmaßnahmen gemäß § 15 RKEG dienen nicht dem allgemeinen Schutz der Einrichtung als Unternehmen, sondern der Aufrechterhaltung der Fähigkeit, den wesentlichen Dienst zu erbringen. Ebenso sind die Grundsätze der Geeignetheit und Verhältnismäßigkeit, der Konformitätsvermutung einschließlich der Begründung bei Abweichungen, des Verhältnisses zu Normen und Richtlinien sowie der Stufenlogik der behördlichen Prüfung, wie in Leitfaden Z 0 dargelegt, zu beachten. Dem risikobasierten Ansatz folgend liegt die konkrete Ausgestaltung bei der kritischen Einrichtung selbst.

Es ist Aufgabe der kritischen Einrichtung, in einem Resilienzplan nachvollziehbar darzulegen, wie sie den Anforderungen im Einzelnen entspricht: welche kritischen Funktionen identifiziert wurden, welche Personalkategorien welchen Sicherheitsvorkehrungen unterliegen, wie Zugangsberechtigungen gesteuert werden, welche Überprüfungen vorgesehen sind und welche Ausbildungs- und Qualifikationsanforderungen gelten.

Der Resilienzplan soll die personellen Sicherheitsvorkehrungen als dauerhaftes, lebendiges System darstellen. Änderungen in der Organisationsstruktur, bei externen Dienstleistungsverhältnissen, in der Bedrohungslage oder im Leistungsumfang des wesentlichen Dienstes sollen zeitnah in die Maßnahmen und deren Dokumentation einfließen.


TECH COMPANY
TECH COMPANY

Z 6: Sensibilisierung und Schulung

1 Allgemeine Grundlagen

2 Schulungsmaßnahmen

3 Informationsmaterialien und Kommunikation

4 Übungen

5 Abschließende Vorgaben

1 Allgemeine Grundlagen

Kritische Einrichtungen haben das Personal in kritischen Funktionen, insbesondere im Rahmen der Bereitstellung von Schulungsmaßnahmen im Hinblick auf die Steigerung der Resilienz, zu sensibilisieren. Sensibilisierung ist eine querschnittsbezogene Maßnahme, die alle Phasen des Resilienzkreislaufs durchzieht und das Fundament dafür bildet, dass technische, organisatorische und personelle Sicherheitsvorkehrungen im Ernstfall tatsächlich wirksam werden.

Ein wirksames Awareness-Programm ist von zentraler Bedeutung, da Personal ein unerlässliches Element in jedem Schritt des Resilienzkreislaufs ist – von der Verhinderung von Sicherheitsvorfällen und der Minderung von Insider-Bedrohungen über die Reaktion auf Sicherheitsvorfälle durch Aktivierung der einschlägigen Verfahren, die Meldung von Sicherheitsvorfällen und die Sicherstellung der Betriebskontinuität bis hin zur Wiederaufnahme des Betriebs nach Wiederherstellung des Zustands vor dem Sicherheitsvorfall. Ohne sachkundiges Personal können selbst die besten technischen und organisatorischen Maßnahmen nur scheitern.

Durch die Sensibilisierung für Resilienzmaßnahmen wird eine Resilienzkultur geschaffen. Diese gewährleistet, dass Resilienz als gemeinsamer Wert der Mitarbeitenden verstanden wird und somit dazu beiträgt, das Risiko von Insider-Bedrohungen oder Social Engineering zu verringern. Eine solche Kultur entsteht nicht durch einzelne Schulungsveranstaltungen, sondern durch ein kohärentes, dauerhaftes Programm aus Schulungen, Informationsmaterialien und Übungen.

Der vorliegende Leitfaden Z 6 behandelt die konkrete Umsetzung der Sensibilisierung: Schulungsmaßnahmen, Informationsmaterialien und Übungen. Die strukturelle Festlegung, welche Qualifikationen für welche Rollen erforderlich sind, ist Gegenstand des Leitfadens Z 5, Kapitel 5. Der vorliegende Leitfaden Z 6 setzt dort an, wo die Anforderungen definiert sind, und beschreibt, wie diese durch konkrete Formate umgesetzt werden.

Vernetzend mit der NIS-2-Richtlinie ist festzuhalten, dass die Sensibilisierungsmaßnahmen kohärent ausgestaltet sein sollen. Bestehende Cyber-Awareness-Programme sollen, soweit möglich, in das Resilienz-Awareness-Programm integriert und nicht parallel aufgebaut werden.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖNORM EN ISO 22301	Sicherheit und Resilienz – Business Continuity Management System – Anforderungen (Kap. 7.3)
ISO 22316	Security and resilience – Organizational resilience – Principles and attributes
ÖVE/ÖNORM EN ISO/IEC 27002	Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Informationssicherheitsmaßnahmen (Kap. 6.3)

Stand: 01. Juni 2026

Tipps

Der häufigste Fehler bei Awareness-Programmen ist deren Reduktion auf eine jährliche Pflichtschulung. Wirksame Sensibilisierung entsteht durch eine Kombination aus regelmäßigen Schulungen, permanent verfügbare Informationsmaterialien und wiederkehrenden Übungen und nicht durch Einzelmaßnahmen.
Die Integration von Resilienz-Awareness- und Cyber-Awareness-Maßnahmen in ein gemeinsames Programm spart nicht nur Ressourcen, sondern vermeidet auch widersprüchliche Botschaften an das Personal. In vielen Bedrohungsszenarien überschneiden sich physische und digitale Angriffsvektoren.

2 Schulungsmaßnahmen

Die von der kritischen Einrichtung organisierten Schulungen sollen die in Leitfaden Z 5, Kapitel 5 definierten Qualifikationsanforderungen in konkrete Lernformate und -inhalte überführen. Schulungen sollen den gesamten Resilienzkreislauf umfassen. Das bedeutet, dass durch die Schulungsinhalte die gesamte Breite der Resilienzmaßnahmen abgedeckt werden sollen: Verhinderung von Sicherheitsvorfällen, physischer Schutz, Abwehr und Bewältigung von Sicherheitsvorfällen, Kontinuität und Wiederaufnahme nach Sicherheitsvorfällen und personelle Sicherheitsvorkehrungen.

Inhaltlich sollen Schulungen insbesondere folgende Schwerpunkte abdecken: das Verständnis der Bedrohungslandschaft; die Rolle der kritischen Einrichtung bei der Aufrechterhaltung lebenswichtiger gesellschaftlicher Funktionen und die schwerwiegenden Folgen von Unterbrechungen der wesentlichen Dienste; das zeitnahe Erkennen und Melden von verdächtigen Aktivitäten, Schwachstellen oder ungewöhnlichen Vorfällen sowie die Reaktion auf und Bewältigung von Sicherheitsvorfällen. Diese Inhalte sollen das Personal in die Lage versetzen, in seinem jeweiligen Aufgabenbereich einen aktiven Beitrag zur Resilienz zu leisten – nicht nur durch regelkonformes Verhalten, sondern auch durch eigenständiges Erkennen und Handeln.

Funktionsspezifische Schulungen für Personal in kritischen Funktionen sollen sichergestellt werden.

Schulungen sollen nicht als einmalige Veranstaltungen konzipiert werden, sondern als wiederkehrendes Programm mit klaren Zyklen, Zielgruppen und Nachweismechanismen. Bei Eintritt oder bei Wechsel in eine neue Funktion sollen Erstschulungen vorgesehen werden. Folgeschulungen sollen in regelmäßigen Abständen (beispielsweise nach Sicherheitsvorfällen, Änderungen der Bedrohungslage oder Anpassungen des Resilienzplans) durchgeführt werden. Die Wirksamkeit der Schulungen soll überprüft werden, um den tatsächlichen Wissenstransfer zu bewerten.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖNORM EN ISO 22361	Sicherheit und Resilienz – Krisenmanagement – Leitlinien (Kap. 9.3)
ISO/TS 22330	Security and resilience – Business continuity management systems – Guidelines for people aspects of business continuity (Kap. 5.4; Kap. 6.5)
ÖNORM EN 17483-1	Private Sicherheitsdienstleistungen – Schutz kritischer Infrastrukturen – Teil 1: Allgemeine Anforderungen (Kap. 6.3)
ÖNORM ISO 10015	Qualitätsmanagement – Leitfaden für Kompetenzmanagement und Personalentwicklung (Kap. 4.2; Kap. 5)
ÖVE/ÖNORM EN ISO/IEC 27002	Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Informationssicherheitsmaßnahmen (Kap. 6.3)

Stand: 01. Juni 2026

Tipps

Die Wirksamkeit von Schulungen soll nicht nur durch Teilnahmelisten, sondern auch durch geeignete Wissensüberprüfungen bewertet werden – etwa durch kurze Tests, Szenarien oder Reflexionsfragen am Ende der Schulung.

Schulungsinhalte sollen regelmäßig an geänderte Bedrohungslagen, neue Resilienzmaßnahmen und Erkenntnisse aus Sicherheitsvorfällen oder Übungen angepasst werden. Statische Schulungsunterlagen, die über Jahre unverändert bleiben, verlieren rasch an Relevanz.

Bei der Schulung externen Personals soll nicht darauf vertraut werden, dass der Dienstleister alle standortspezifischen Inhalte abdeckt. Standortspezifische Einweisungen – insbesondere zu Notfallplänen, Flucht- und Rettungswegen, Gefahrenbereichen und Meldeabläufen – sollen von der kritischen Einrichtung selbst sichergestellt werden.

3 Informationsmaterialien und Kommunikation

Neben Schulungen bilden Informationsmaterialien ein wesentliches Instrument der laufenden Sensibilisierung. Sie ermöglichen es, zentrale Inhalte dauerhaft und niederschwellig zugänglich zu machen, ohne dass dafür jedes Mal eine formale Schulungsveranstaltung erforderlich ist.

Informationsmaterialien, die dem Personal zur Verfügung gestellt werden, sollen direkt mit der unternehmensinternen Risikoanalyse und den getroffenen Resilienzmaßnahmen der kritischen Einrichtung verknüpft sein. Diese Informationsmaterialien sollen klar und leicht verständlich sein und die kritische Rolle der kritischen Einrichtung sowie die Auswirkungen von Sicherheitsvorfällen auf Gesellschaft und Wirtschaft, den All-Gefahren-Ansatz und die zentralen Sicherheitsprinzipien wie „See something – say something" sowie das Prinzip der geringsten Privilegien/das Prinzip der minimalen Rechtevergabe für den Zugang zu sensiblen Informationen erläutern. Daraus folgt, dass generische, nicht auf die kritische Einrichtung zugeschnittene Materialien für die Sensibilisierung nicht ausreichend sind. Die Materialien sollen konkret auf die Bedrohungslage, die Schutzgüter und die Resilienzmaßnahmen der jeweiligen kritischen Einrichtung Bezug nehmen.

Sensibilisierungsmaterialien sollen so aufbereitet sein, dass sie im Arbeitsalltag unmittelbar nutzbar sind. Visuelle Materialien zum schnellen Nachschlagen – etwa zu physischen Sicherheitsverletzungen, Strom- oder Konnektivitätsausfällen oder dem Fund verdächtiger Pakete – können die Handlungssicherheit des Personals im Ereignisfall wesentlich stärken. Ergänzend sollen Ablaufdiagramme zur Meldung von Sicherheitsvorfällen und Richtlinien zum physischen Schutz sowie zur Zutrittskontrolle in leicht zugänglicher Form aufbereitet werden. Um die Sensibilisierung zu maximieren, sollen diese Materialien in mehreren Formaten bereitgestellt werden – digital, physisch und interaktiv.

Digitale Formate umfassen insbesondere Intranet-Seiten, verpflichtende E-Learning-Module mit Wissensüberprüfungen, Kurzvideos und Bildschirmschoner mit zentralen Sicherheitsbotschaften. Physische Formate umfassen Poster, Informationsblätter und Quick-Reference-Karten. Interaktive Formate umfassen insbesondere FAQ-Seiten, bei denen das Personal eigenständig Antworten auf häufige Fragen findet. Die Auswahl der Formate soll sich an der Arbeitsumgebung, der Erreichbarkeit des Personals und der Art der zu vermittelnden Inhalte orientieren.

Informationsmaterialien sollen regelmäßig auf Aktualität und Relevanz überprüft und bei geänderter Bedrohungslage, an neue Resilienzmaßnahmen oder Erkenntnisse aus Vorfällen und Übungen angepasst werden.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ÖVE/ÖNORM EN ISO/IEC 27002	Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Informationssicherheitsmaßnahmen (Kap. 6.3)
ÖNORM EN ISO 22301	Sicherheit und Resilienz – Business Continuity Management System – Anforderungen (Kap 7.4)

Stand: 01. Juni 2026

Tipps

Informationsmaterialien sollen dort platziert werden, wo das Personal sie im Alltag tatsächlich wahrnimmt: an Zugangspunkten, in Aufenthaltsräumen, auf digitalen Arbeitsflächen. Material, das nur in einem Intranet-Archiv abgelegt wird, erreicht in der Praxis wenige Personen.
Übersichtliche Kurzanleitungen zur Meldung von Sicherheitsvorfällen gehören zu den wirksamsten Awareness-Instrumenten: Sie beantworten die für das Personal im Ernstfall entscheidende Fragen (wen rufe ich an, was sage ich, was tue ich bis Hilfe kommt) in wenigen Sekunden. Bewährt hat sich dabei die Methode der Quick-Reference-Cards.
Quick-Reference-Karten im Scheckkartenformat für Notfallnummern, Sammelplätze und Erstmaßnahmen können vom Personal ständig mitgeführt werden und sind bei einem Sicherheitsvorfall schneller verfügbar als jedes digitale System.

4 Übungen

Übungen sind ein zentrales Instrument der Sensibilisierung und der Validierung des Resilienzplans. Sie versetzen das Personal in die Lage, die in Schulungen und Informationsmaterialien vermittelten Inhalte unter realistischen Bedingungen anzuwenden, und machen erkennbar, wo Verfahren, Rollen, Kommunikationswege oder Ressourcen im Ernstfall tatsächlich belastbar sind.

Der vorliegende Leitfaden Z 6 behandelt Übungen aus der Perspektive der Sensibilisierung: Wie tragen Übungen dazu bei, das Bewusstsein, die Handlungsfähigkeit und die Resilienzkultur zu stärken? Die operative Validierung der Bewältigungsfähigkeit wird im Leitfaden Z 3 behandelt, die Business-Continuity-Management-Tests im Leitfaden Z 4. Auf eine inhaltliche Wiederholung wird daher verzichtet.

Für die Auswahl von Übungsformaten stehen verschiedene Übungstypen, wie beispielsweise Planbesprechungen und Stabsübungen oder praktische Übungen, zur Verfügung. Planbesprechungen und Stabsübungen testen Koordinations-, Entscheidungs- und Kommunikationsprozesse anhand eines simulierten Sicherheitsvorfalls – etwa eines schwerwiegenden Infrastrukturausfalls, eines längeren Stromausfalls oder einer internen Sicherheitsverletzung. Praktische Übungen testen ein spezifisches, zeitkriti-

sches Verfahren – etwa die Aktivierung des Notstromaggregats, die Evakuierung eines kritischen Bereichs oder die Isolierung einer kompromittierten Steuerungskomponente.

Bei der Organisation von Übungen sollen kritische Einrichtungen den Fokus auf die Ergebnisse ihrer einrichtungsinternen Risikoanalyse legen, den gesamten Resilienzkreislauf testen und – sofern relevant – eine gute sektorübergreifende Koordination mit anderen kritischen Einrichtungen gewährleisten, um sektorübergreifende Abhängigkeiten zu testen. Sie sollen im Falle von Sicherheitsvorfällen die Zusammenarbeit mit relevanten Behörden wie Strafverfolgungsbehörden und Einsatzkräften wie z.B. Feuerwehr und sonstigen Rettungsdiensten sicherstellen und diese in die Übungen einbinden.

Übungen sollen nicht als isolierte Einzelereignisse, sondern als wiederkehrendes Programm gestaltet werden. Der Übungsplan soll eine angemessene Kombination aus Tabletop- und praktischen Übungen vorsehen und dabei unterschiedliche Szenarien und Funktionsbereiche abdecken. Die Übungsszenarien sollen auf den Ergebnissen der einrichtungsinternen Risikoanalyse aufbauen und regelmäßig angepasst werden. Erkenntnisse aus Übungen sollen systematisch dokumentiert und in die Verbesserung von Verfahren, Schulungsinhalten und Resilienzmaßnahmen überführt werden.

Beispiele für unterstützende Normen und Richtlinien

Bezeichnung	*Spezifische Inhalte*
ISO 22398	Societal security – Guidelines for exercises (Kap. 4; Kap. 5; Kap. 6)
ÖNORM EN ISO 22361	Sicherheit und Resilienz – Krisenmanagement – Leitlinien (Kap. 9.4; Kap.9.5; Kap. 9.6)
ÖNORM D 4902-3	Risikomanagement für Organisationen und Systeme – Leitfaden – Teil 3: Notfall-, Krisen- und Kontinuitätsmanagement – Anleitung zur Umsetzung der ISO 31000
ÖNORM EN ISO 22301	Sicherheit und Resilienz – Business Continuity Management System – Anforderungen (Kap. 8.5)

Stand: 01. Juni 2026

Tipps

Tabletop-Übungen sind ressourcenschonend und können innerhalb wenigen Stunden durchgeführt werden. Sie eignen sich besonders für die Sensibilisierung von Führungskräften und Entscheidungsträgern, die selten in operative/praktische Übungen eingebunden werden.
Praktische Übungen sollen nicht nur technische Abläufe testen, sondern auch die Frage beantworten, ob das Personal die Verfahren kennt, die richtigen Ansprechpersonen erreicht und unter Stress handlungsfähig ist.
Die Einbindung von Behörden und Ersteinsatzkräften in Übungen erfordert

eine frühzeitige Abstimmung. Es soll vorab geklärt werden, welche Behörden einzubinden sind, welche Szenarien geeignet sind und wie die Kommunikation im Übungsfall organisiert wird. Ein Telefonkontakt wenige Tage vor der Übung reicht dafür nicht aus.
Übungen entfalten ihren Mehrwert erst durch eine strukturierte Nachbereitung. Dabei ist zwischen „lessons identified" – also den unmittelbar nach der Übung festgehaltenen Beobachtungen und Schwachstellen – und „lessons learned" zu unterscheiden, die erst dann entstehen, wenn Erkenntnisse tatsächlich in Verbesserungsmaßnahmen überführt und umgesetzt wurden. Nur was nachweislich geändert wurde, ist gelernt.
Erkenntnisse aus Übungen sollen nicht nur dokumentiert, sondern nachweisbar in konkrete Weiterentwicklungen überführt werden. Ein Maßnahmenplan mit Verantwortlichkeiten und Fristen stellt sicher, dass identifizierte Schwächen nicht bis zur nächsten Übung unbearbeitet bleiben.

5 Abschließende Vorgaben

Für die Umsetzung des Leitfadens Z 6 wird nochmals darauf hingewiesen, dass sämtliche Anforderungen auf den wesentlichen Dienst der kritischen Einrichtung bezogen sind. Die Resilienzmaßnahmen gemäß § 15 RKEG dienen nicht dem allgemeinen Schutz der Einrichtung als Unternehmen, sondern der Aufrechterhaltung der Fähigkeit, den wesentlichen Dienst zu erbringen. Ebenso sind die Grundsätze der Geeignetheit und Verhältnismäßigkeit, der Konformitätsvermutung einschließlich der Begründung bei Abweichungen, des Verhältnisses zu Normen und Richtlinien sowie der Stufenlogik der behördlichen Prüfung, wie im Leitfaden Z 0 dargelegt, zu beachten. Dem risikobasierten Ansatz folgend liegt die konkrete Ausgestaltung bei der kritischen Einrichtung selbst.

Es ist die Aufgabe der kritischen Einrichtung, in einem Resilienzplan nachvollziehbar darzulegen, wie sie den Anforderungen im Einzelnen entspricht: welche Schulungsmaßnahmen für welche Personalkategorien vorgesehen sind, welche Informationsmaterialien bereitgestellt werden, wie das Übungsprogramm aufgebaut ist und wie die Wirksamkeit der Maßnahmen überprüft wird.

Der Resilienzplan soll Sensibilisierung und Schulung als dauerhaften, lebendigen Prozess etablieren. Schulungsinhalte, Informationsmaterialien und Übungsprogramme sollen regelmäßig auf ihre Aktualität, Relevanz und Wirksamkeit überprüft und bei geänderter Bedrohungslage oder organisatorischen Veränderungen sowie an neue Resilienzmaßnahmen oder Erkenntnisse aus Sicherheitsvorfällen und Übungen angepasst werden.

Notizen

Notizen

Notizen