Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Bundesamt für Bevölkerungsschutz BABS

Leitfaden Schutz kritischer Infrastrukturen

Impressum

Herausgeber

Bundesamt für Bevölkerungsschutz
Monbijoustrasse 51a
3003 Bern

Das Bundesamt für Bevölkerungsschutz dankt für allfällige Anregungen und Rückmeldungen. Sie erreichen uns über die E-Mail-Adresse ski@babs.admin.ch

Weitere Informationen zum Schutz kritischer Infrastrukturen finden Sie auf unserer Website www.infra-protection.ch

Versionskontrolle

Version	Datum	Beschreibung
1.0	30.5.2015	
1.1	17.12.2018	Anpassung Skalierung der Schadensklassen; diverse redaktionelle Änderungen (insb. in Bezug auf aktualisierte SKI-Strategie)

Disclaimer

Der Leitfaden basiert auf gängigen Normen und Standards im Bereich Risiko-, Notfall-, Krisen- und Kontinuitätsmanagement und führt diese zu einem integralen Ansatz zum Schutz kritischer Infrastrukturen zusammen. Die Empfehlungen entsprechen dem Stand der Kenntnisse zum Zeitpunkt der Erstellung des Dokuments. Sie können aufgrund künftiger Entwicklungen überholt sein, ohne dass das Dokument in der Zwischenzeit geändert wurde. Der Leitfaden ist seitens des Bundesamts für Bevölkerungsschutz BABS rechtlich nicht bindend. Das BABS achtet mit aller Sorgfalt auf die Richtigkeit veröffentlichter Informationen. Nichtsdestotrotz kann es hinsichtlich der inhaltlichen Aktualität und Vollständigkeit dieses Dokumentes keine Gewährleistung übernehmen. Haftungsansprüche wegen Schäden materieller und immaterieller Art durch die Nutzung bzw. Nichtnutzung der veröffentlichten Informationen werden daher ausgeschlossen.

Inhaltsverzeichnis

Zusammenfassung

Als kritische Infrastrukturen (KI) werden Versorgungssysteme, Prozesse und Einrichtungen bezeichnet, die essenziell für das Funktionieren der Wirtschaft oder das Wohlergehen der Bevölkerung sind. Dazu zählen etwa die Energieversorgung, der Personen- und Güterverkehr oder die medizinische Versorgung. Schwerwiegende Ausfälle der Stromversorgung, des Schienenverkehrs oder der Lebensmittelversorgung könnten gravierende Schäden verursachen. Eines der Hauptziele der nationalen Strategie zum Schutz kritischer Infrastrukturen, die der Bundesrat im Juni 2012 verabschiedet und 2017 aktualisiert hat, ist die Überprüfung und Verbesserung der Resilienz (Widerstands- und Regenerationsfähigkeit) der kritischen Infrastrukturen an und für sich. Der vorliegende Leitfaden beschreibt das entsprechende Vorgehen.

Übergeordneter Zweck des Leitfadens ist es, schwerwiegende Ausfälle nach Möglichkeit verhindern respektive im Ereignisfall die Ausfallzeit reduzieren zu helfen. Mit dem Leitfaden soll überdies zu einem verbesserten Umgang und Verständnis in Zusammenhang mit den zu erwartenden Risiken beigetragen werden.

Methodisch orientiert sich der Leitfaden an gängigen und etablierten Konzepten des Risiko-, Krisen- und Kontinuitätsmanagements und kombiniert verschiedene Elemente dieser Ansätze im Sinne eines *integralen Schutzes*. Der Leitfaden baut auf Planungen und Arbeiten auf, die auf Ebene der Unternehmen vielerorts bereits existieren. Während diese in der Regel auf Risiken *für das Unternehmen* fokussieren, steht beim Schutz kritischer Infrastrukturen die Frage im Vordergrund, inwiefern *die Bevölkerung und ihre (wirtschaftlichen) Lebensgrundlagen* durch Ausfälle von bzw. Störungen bei kritischen Infrastrukturen beeinträchtigt werden.

Der Leitfaden soll dabei behilflich sein, die entsprechenden Risiken zu überprüfen und allfällige Lücken zu identifizieren. Dabei hat der Leitfaden nicht die Absicht, einen vollumfänglichen und unverhältnismässigen Schutz gegen sämtliche Gefährdungen zu erwirken.

Der Leitfaden verfolgt vielmehr einen risikobasierten Ansatz, der zum Ziel hat, dass die Kosten von allenfalls zusätzlich notwendigen Massnahmen in einem positiven Verhältnis zu deren Nutzen stehen. Dieser Ansatz soll ausserdem dazu beitragen, Ungleichbehandlungen oder Marktverzerrungen innerhalb oder zwischen den einzelnen Branchen zu verhindern.

Die Umsetzung des SKI-Leitfadens erfordert in der Regel eine enge Zusammenarbeit zwischen den Betreibern der kritischen Infrastrukturen und den jeweiligen Fach-, Aufsichts- und Regulationsbehörden auf den Ebenen Bund, Kantone oder Gemeinden. Diese sind in ihren jeweiligen Zuständigkeitsbereichen dafür verantwortlich, die Rahmenbedingungen für das Funktionieren der kritischen Infrastrukturen zu gestalten. In den verschiedenen Politikbereichen (Energiepolitik, Verkehrspolitik, Gesundheitswesen usw.) wird ebenfalls die Umsetzung und Finanzierung der unter Umständen notwendigen zusätzlichen Schutzmassnahmen zu klären sein.

Es ist indes für die Betreiber auch möglich, den Leitfaden ohne Einbezug der Behörden anzuwenden. Der Leitfaden kann den Unternehmen behilflich sein zu überprüfen, ob allenfalls Risiken in Bezug auf gravierende Ausfälle bestehen, die nicht zuletzt auch eine existenzielle Gefahr für den Fortbestand des Betriebs darstellen könnten.

1 Einleitung

1.1 Ausgangslage

Kritische Infrastrukturen

Kritische Infrastrukturen[1] (KI) stellen die Verfügbarkeit von wichtigen Gütern und Dienstleistungen wie Energie, Kommunikation oder Verkehr sicher. Störungen, Ausfälle oder die Zerstörung von kritischen Infrastrukturen können schwerwiegende Auswirkungen auf die Bevölkerung und ihre Lebensgrundlagen haben.

Die kritischen Infrastrukturen werden in sogenannte Sektoren und Teilsektoren unterteilt (z. B. Stromversorgung, Erdölversorgung und Erdgasversorgung im Sektor Energie).[2] Innerhalb der kritischen Teilsektoren sind grundsätzlich *sämtliche* Elemente oder Objekte (z. B. Betreiberfirmen, Anlagen, Systeme usw.) Bestandteil der kritischen Infrastruktur, wobei sich die jeweilige Bedeutung (oder Kritikalität) selbstverständlich unterscheidet.[3]

Nationale SKI-Strategie

Am 8. Dezember 2017 hat der Bundesrat die nationale Strategie zum Schutz kritischer Infrastrukturen (SKI) 2018 – 2022 verabschiedet.[4] Diese ersetzt die nationale SKI-Strategie von 2012. Die nationale SKI-Strategie 2018 – 2022 hält die übergeordneten Grundsätze, Definitionen, Ziele und Massnahmen für einen umfassenden Schutz der Schweiz im Hinblick auf kritische Infrastrukturen fest. Sie dient allen involvierten Stellen auf den Ebenen Bund, Kantone, Gemeinden und KI-Betreiber als Bezugsrahmen für ihre spezifischen Arbeiten im SKI-Bereich.

Die Strategie bezeichnet insgesamt 17 Massnahmen, unter anderem etwa die Führung eines periodisch aktualisierten Inventars der kritischen Infrastrukturen (SKI-Inventar). Weitere Massnahmen betreffen beispielsweise die Erarbeitung von vorsorglichen Einsatzplanungen durch die Partner im Bevölkerungsschutz und die Armee. Ein Hauptschwerpunkt der Strategie stellt die Überprüfung und Verbesserung der Resilienz der kritischen Infrastrukturen an und für sich dar. Zu diesem Zweck hat der Bundesrat mit Massnahme M1 die Betreiber der kritischen Infrastrukturen beauftragt, ihre Resilienz (Widerstands und Regenerationsfähigkeit) zu überprüfen und bei Bedarf zu verbessern. Der vorliegende Leitfaden zeigt auf, welche Punkte dabei zu berücksichtigen sind und wie vorzugehen ist. In Ergänzung zu den Arbeiten auf Ebene der Betreiber hat der Bundesrat die zuständigen Fach-, Aufsichts- und Regulierungsbehörden in den verschiedenen Sektoren beauftragt, in allen Teilsektoren zu prüfen, ob Risiken für schwerwiegende Ausfälle bestehen und bei Bedarf Massnahmen zu treffen, um diese Risiken zu reduzieren. Dabei kommt ein Vorgehen zur Anwendung, das sich eng an demjenigen des SKI-Leitfadens orientiert.

Vorarbeiten

In verschiedenen Teilsektoren existieren bereits Vorgaben und Planungen zum Schutz der kritischen Infrastrukturen. Diese beziehen sich in der Regel jedoch nur auf einzelne Aspekte (z. B. Schutz vor von Infrastrukturen ausgehenden Gefahren, Produktsicherheit, langfristige Versorgungssicherheit, Schutz vor einzelnen Gefährdungen usw.). Der Leitfaden berücksichtigt demgegenüber im Sinne des *integralen Schutzes* sowohl ein umfassendes Gefährdungsspektrum wie auch ein umfassendes Massnahmenspektrum. Dies bedeutet, dass sämtliche *relevanten* Gefährdungen, die zu Ausfällen oder Störungen führen können, zu betrachten sind.

---

[1] Für eine ausführliche Begriffserklärung siehe → Begriffserläuterungen.

[2] Zum Überblick vgl. Anhang 7 – Kritische Sektoren und Teilsektoren.

[3] Dementsprechend ist innerhalb der Teilsektoren keine Unterscheidung zwischen kritisch oder nicht kritisch möglich. Im Teilsektor Stromversorgung sind beispielsweise grundsätzlich sämtliche rund 900 Elektrizitätsversorgungsunternehmen als KI-Betreiber zu betrachten, wobei die Bedeutung selbstverständlich unterschiedlich ist: Einige sind auf nationaler Ebene relevant, (viele) andere dagegen lediglich auf kommunaler oder lokaler Ebene.

[4] Die Nationale Strategie zum Schutz kritischer Infrastrukturen 2018-2022 (BBl 2018 503) ist auf der SKI-Website www.infraprotection.ch verfügbar.

Das Massnahmenspektrum beinhaltet sämtliche *geeigneten* baulichen, technischen und organisatorischen Massnahmen, um Ausfälle zu verhindern oder im Ereignisfall die Ausfallzeit zu reduzieren. Auch die KI-Betreiber verfügen in der Regel über umfassende Planungen in Bezug auf den Schutz und die Sicherheit ihres Unternehmens. So sind viele gemäss Obligationen-, Unternehmens- oder Aktienrecht sogar verpflichtet, ein wirksames Risikomanagement bzw. ein internes Kontrollsystem (IKS) zu führen. Viele Unternehmen verfügen zudem über Planungen zur Sicherstellung der Betriebskontinuität (Business Continuity Management BCM). Der vorliegende Leitfaden ist so gestaltet, dass er sich methodisch an diesen Prozessen orientiert und gewährleistet, dass entsprechende Arbeiten berücksichtigt werden können (vgl. Kapitel 2). Damit kann der Aufwand für Unternehmen erheblich reduziert werden. Bereits bestehende Vorgaben, Vereinbarungen, Massnahmen usw. werden im Rahmen der Vorarbeiten gezielt erfasst (vgl. Kapitel 3.1.3) und bei der Risikoanalyse berücksichtigt. Sind bereits zahlreiche Sicherheitsmassnahmen implementiert, wird sich dies durch entsprechend geringere Risiken manifestieren. Dadurch wird auch der Handlungsbedarf in Bezug auf zusätzliche Massnahmen reduziert.

1.2 Leitfaden SKI

Entstehung

Der Leitfaden wurde in enger Zusammenarbeit mit der interdepartementalen Arbeitsgruppe SKI (AG SKI)[5], in welcher 26 Bundesstellen und zwei Kantone vertreten sind, ausgearbeitet. Die Erarbeitung des Leitfadens wurde von einer Kerngruppe begleitet, die sich aus Experten in den Bereichen Risiko-, Notfall-, Krisen- und Kontinuitätsmanagement zusammensetzte. Im September 2011 fand zudem unter Mitwirkung der ETH Zürich ein Workshop statt, in dem der Leitfaden durch Experten in den oben genannten Bereichen sowie von Vertretern aus der Privatwirtschaft, der Wissenschaft und Verbänden getestet und evaluiert wurde.

In den Jahren 2012 und 2013 wurde der Leitfaden in Zusammenarbeit mit einem KI-Betreiber zuerst an einem konkreten KI-Objekt überprüft und später während mehrerer Monate über die wichtigsten Unternehmensprozesse auf seine Praxistauglichkeit getestet. Im Frühling 2014 wurde der Leitfaden schliesslich bei Fachverbänden, KI-Betreibern, kantonalen Konferenzen sowie erneut bei der AG SKI einer fachlichen Konsultation unterzogen.

Ziel und Zweck

Der vorliegende *Leitfaden Schutz kritischer Infrastrukturen* stellt ein Instrument zur Überprüfung und gegebenenfalls Verbesserung der Resilienz der kritischen Infrastrukturen dar. Insbesondere ist er konzipiert im Hinblick auf die Anwendung auf Ebene der kritischen Teilsektoren sowie auf Stufe Betrieb oder Objekte des SKI-Inventars[6].

Der Leitfaden soll dazu beitragen, die Wahrscheinlichkeit von grossflächigen und länger andauernden Störungen oder Ausfällen von KI zu reduzieren sowie das Schadensausmass und die Ausfallzeit im Ereignisfall zu begrenzen. Ziel ist es, dass jede KI optimal geschützt ist – das heisst, dass Massnahmen umgesetzt sind, die adäquat sind zum Risiko, welches die KI

[5] Bundesstellen: Bundeskanzlei BK, Abteilung Sicherheitspolitik ASP-EDA, Direktion für Entwicklung und Zusammenarbeit DEZA, Bundesamt für Gesundheit BAG, Bundesamt für Meteorologie und Klimatologie MeteoSchweiz, Bundesamt für Polizei fedpol, Sicherheitspolitik VBS SIPOL VBS, Nachrichtendienst des Bundes NDB, Informations- und Objektsicherheit IOS, Kommando Operationen, armasuisse Immobilien ar Immo, Bundesamt für Bevölkerungsschutz BABS, Eidgenössische Finanzverwaltung EFV, Bundesamt für Bauten und Logistik BBL, Bundesamt für Informatik und Telekommunikation BIT, Informatiksteuerungsorgan Bund ISB (Koordinationsstelle nationale Strategie Cyber-Risiken), Bundesamt für wirtschaftliche Landesversorgung BWL, Bundesamt für Verkehr BAV, Bundesamt für Zivilluftfahrt BAZL, Bundesamt für Energie BFE, Bundesamt für Strassen ASTRA, Bundesamt für Kommunikation BAKOM, Bundesamt für Umwelt BAFU, Eidgenössische Elektrizitätskommission ElCom, Eidgenössisches Nuklearsicherheitsinspektorat ENSI.
Kantone: Kanton Genf, Kanton Basel-Stadt.

[6] Im SKI-Inventar sind Objekte aufgeführt, die von strategisch wichtiger Bedeutung für die Schweiz sind. Das SKI-Inventar ermöglicht unter anderem eine vergleichende Übersicht über die Bedeutung der Objekte. Es dient als Planungs- und Entscheidungsgrundlage im Risiko-, Krisen- und Katastrophenmanagement auf den Stufen Bund, Kantone und Betreiber. Das SKI-Inventar ist in seiner Gesamtheit als GEHEIM klassifiziert, einzelne Auszüge sind in der Regel VERTRAULICH klassifiziert.

darstellen. Nicht angestrebt wird hingegen ein vollumfänglicher Schutz im Hinblick auf sämtliche Risiken – dies würde den Prinzipien des risikobasierten Vorgehens und der Verhältnismässigkeit widersprechen, die in der nationalen SKI-Strategie vorgegeben wurden.

Der Leitfaden soll überdies auch zu einem verbesserten Umgang mit und Verständnis von den zu erwartenden Risiken beitragen. Die mit Hilfe des Leitfadens gewonnenen Erkenntnisse sollen weiter für die Ergänzung von eventuell fehlenden bzw. unzureichenden Schutzmassnahmen genutzt und in den bestehenden betriebsinternen Strukturen des Risiko-, Notfall-, Krisen- und Kontinuitätsmanagements berücksichtigt werden.

Adressaten

Der Schutz kritischer Infrastrukturen ist eine Gemeinschaftsaufgabe, die eine enge Zusammenarbeit zwischen den KI-Betreibern und den jeweils zuständigen Fach-, Aufsichts- und Regulierungsbehörden verlangt. Der Leitfaden richtet sich deshalb sowohl an die KI-Betreiber als auch an die jeweils verantwortlichen Behörden. Die Umsetzung des Leitfadens kann demzufolge initiiert werden durch:

1. KI-Betreiber, die dafür verantwortlich sind, ein möglichst kontinuierliches Funktionieren ihrer Anlagen sicherzustellen, und die den Leitfaden in Eigenverantwortung umsetzen wollen.
2. Fachbehörden auf den Ebenen Bund, Kantone oder Gemeinden, welche für die jeweiligen kritischen Infrastrukturen aufgrund gesetzlicher Grundlagen eine Steuerungs- oder Aufsichtsfunktion wahrnehmen. Der Leitfaden kann sie bei der Abklärung unterstützen, ob Risiken für die Gesellschaft und die Wirtschaft bestehen, die gesetzgeberischer, regulatorischer o. ä. Massnahmen seitens der Behörden bedürfen.

Da einzelne Massnahmen zum Schutz der kritischen Infrastrukturen durchaus kostenintensiv sein dürften, wird dringend empfohlen, bei der Umsetzung des Leitfadens und insbesondere bei der Evaluation von möglichen Massnahmen die Zusammenarbeit mit weiteren Betreibern kritischer Infrastrukturen zu suchen. Mit gemeinsam beschafften und genutzten Ressourcen für oder einer verstärkten Kooperation im Ereignisfall (z. B. in Form einer gemeinsamen Krisenorganisation) lassen sich Risiken vielfach kostengünstig und effektiv reduzieren. Eine wichtige Rolle bei der Koordination der Arbeiten können dabei die verschiedenen Branchenverbände einnehmen.

Mehrwert für die KI-Betreiber

Für die KI-Betreiber resultiert durch die Anwendung des Leitfadens auf verschiedenen Ebenen ein Mehrwert in Bezug auf den Schutz der KI:

- Der Leitfaden schafft Entscheidungsgrundlagen für einen effizienten Mitteleinsatz (minimale Investitionen für maximalen Sicherheitsgewinn).
- Der Leitfaden hilft den Betreibern, die Leistungen, die sie zugunsten der Bevölkerung und der Wirtschaft erbringen, zu verdeutlichen und zusammen mit den zuständigen Fachbehörden Massnahmen zur Sicherstellung dieser Leistungen zu evaluieren.
- Der Leitfaden fördert die Unité de doctrine und die Kompatibilität von Massnahmen innerhalb und zwischen den verschiedenen Branchen der kritischen Infrastrukturen in Bezug auf den integralen Schutz.
- Durch eine breite Umsetzung des Leitfadens profitieren die Unternehmen nicht zuletzt selbst von einer weiterhin gewährleisteten, hohen Verfügbarkeit der kritischen Infrastrukturen in der Schweiz (Standortvorteil).

Positionierung

Der Leitfaden ersetzt oder übersteuert keine geltenden Vorgaben in Bezug auf den Schutz von kritischen Infrastrukturen. Er versteht sich als Ergänzung zu bereits vorhandenen oder laufen-

den Arbeiten in diesem Bereich. Der Leitfaden greift methodisch auf bestehende Managementsysteme zurück (vgl. Kapitel 2). Der parallele Aufbau von zusätzlichen Systemen und Werkzeugen soll vermieden werden.

2 Voraussetzungen

2.1 Nahtstellen mit etablierten Managementsystemen

Der Leitfaden weist Nahtstellen mit verschiedenen Managementsystemen auf, die auf Unternehmens-Ebene in der Regel etabliert sind. Dazu gehören beispielsweise:

- Sicherheitsmanagement
- Risikomanagement
- Kontinuitätsmanagement (engl. *Business Continuity Management* BCM)
- Krisenmanagement
- Notfallmanagement
- Internes Kontrollsystem (IKS)

Die genannten Managementsysteme werden in den verschiedenen Standards und Normen und in der Literatur unterschiedlich definiert. Abhängig von der Organisation werden die einzelnen Systeme eigenständig nebeneinander behandelt oder einzelne Systeme werden als Teilsystem in ein anderes integriert. Entscheidend ist, dass jede Komponente verschiedene Aspekte adressiert, die sich gegenseitig sinnvoll ergänzen und die Sicherheit im Unternehmen verbessern, um einen Beitrag zur Minderung der Wahrscheinlichkeit respektive des Ausmasses von Ausfällen zu leisten. Um einen umfassenden Schutz zu etablieren, ist es notwendig, alle Aspekte in der Unternehmenssicherheit zu berücksichtigen. Wie die einzelnen Systeme zusammenspielen, ist durch die Organisation selber zu bestimmen.

Es ist weder Ziel und Anspruch des Leitfadens, eine allgemeingültige Definition der Systeme zu liefern, noch diese abschliessend gegeneinander abzugrenzen. Zum Verständnis des Leitfadens und des Zusammenspiels der verschiedenen Komponenten werden die oben genannten Managementsysteme unter Berücksichtigung ausgewählter Definitionen in den Begriffserläuterungen zu diesem Dokument kurz dargestellt.

Für SKI besonders wichtige Managementsysteme

Von den genannten Managementsystemen sind für SKI insbesondere das Risikomanagement (Aspekt «Verhindern von Ereignissen») und das Kontinuitätsmanagement (Aspekt «Vorbereitung auf Ereignisse») von zentraler Bedeutung. Da verschiedene Definitionen und Auffassungen existieren, wie sich die beiden Managementsysteme definieren bzw. unterscheiden, wird auf eine abschliessende Definition der beiden Ansätze verzichtet. Stattdessen werden nachfolgend die wichtigsten Normen und Richtlinien als Informationsmöglichkeiten für interessierte Stellen aufgeführt.

Themengebiet	Grundlagen
Risikomanagement	*Anleitungen und Hinweise zum Aufbau eines Risikomanagements geben z. B.:* *- ISO 31000 Integriertes Risikomanagement* *- ONR 49001 ff. Umsetzung der ISO 31000 in die Praxis* *- HB 436:2004 Risk Management Guidelines Companion to AS/NZS 4360:2004* *- Handbuch zum Risikomanagement Bund*
Massnahmen zur Sicherstellung der Kontinuität	*Anleitungen und Hinweise zum Aufbau eines Kontinuitätsmanagements geben z. B.:* *- ISO 22301: Societal Security – Business Continuity Management Systems – Requirements* *- ISO 22313: Societal Security – Business Continuity Management Systems – Guidance. First edition, 15. December 2012* *- BS 25999-2* *- BCI Good Practice Guidelines 2013* *- BCM-Ratgeber des Bundesamts für wirtschaftliche Landesversorgung («Unternehmenserfolg nachhaltig sichern – auch im Krisenfall»)* *- HB 221/2004 Business Continuity Management (basiert auf AS/NZS)*

Tabelle 1: Grundlagen-Dokumente pro Themengebiet

2.2 Der Ansatz des Leitfadens

Erweiterung des Blickwinkels

Durch die Anwendung des Leitfadens soll nicht ein weiteres Managementsystem im Unternehmen eingeführt werden. Vielmehr soll auf den bestehenden Systemen aufgebaut und diese um den Blickwinkel des Schutzes kritischer Infrastrukturen erweitert werden: Während der Fokus bei herkömmlichen Managementsystemen auf den Risiken für das Unternehmen bzw. die Organisation liegt, stehen bei SKI die Risiken für die Bevölkerung und ihre Lebensgrundlage im Vordergrund.

*Die **Lebensgrundlage** ist die Gesamtheit der Elemente, die für das Leben der Bevölkerung notwendig sind. Die Lebensgrundlagen ermöglichen das kollektive und individuelle Zusammenleben. Sie lassen sich in natürliche, wirtschaftliche und gesellschaftliche Lebensgrundlagen unterteilen:*

- *Natürliche Lebensgrundlagen:*
  intakte Umwelt (Boden, Wasser, Luft, Biodiversität)
- *Wirtschaftliche Lebensgrundlagen:*
  prosperierende Wirtschaft und funktionierende Infrastrukturen
- *Gesellschaftliche Lebensgrundlagen:*
  funktionierendes Rechtssystem, Gesundheitswesen, Wissenschafts- und Bildungssystem, Vertrauen der Bevölkerung in die staatlichen Institutionen, territoriale Integrität und kulturelle Vielfalt

Beim etablierten (Unternehmens-)Risiko- bzw. Kontinuitätsmanagement stehen Prozesse und Risiken im Vordergrund, die eine wichtige Bedeutung für das (in der Regel wirtschaftliche) Wohlergehen des Unternehmens haben. Demgegenüber fokussiert der SKI-Leitfaden auf Prozesse und Risiken mit wichtiger Bedeutung für die Allgemeinheit. Dabei ist es zwar durchaus möglich, dass es zwischen diesen beiden Aspekten Überschneidungen gibt, vollständig deckungsgleich dürften sie aber nur in den seltensten Fällen sein.

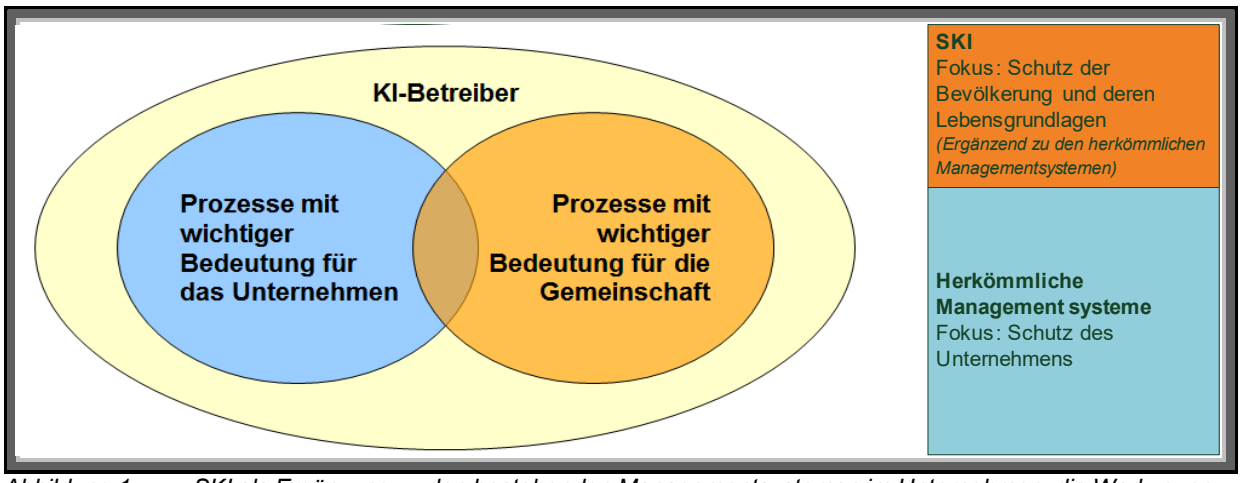


Abbildung 1: SKI als Ergänzung zu den bestehenden Managementsystemen im Unternehmen; die Werkzeuge bleiben die gleichen, die Bezugsebene wird erweitert.

Beispiel: Für viele Unternehmen sind in der Regel Prozesse bzw. Risiken im Bereich des Inkassos von grosser Bedeutung. Die Bevölkerung und die Wirtschaft sind bei einem entsprechenden Ausfall indes nicht unmittelbar betroffen. Demgegenüber kann ein Prozess im Bereich der Grundversorgung aus Sicht des Unternehmens (wirtschaftlich) unbedeutend sein, für die betroffene Wirtschaft und die Bevölkerung aber von zentraler Bedeutung.

Der SKI-Leitfaden stützt sich zwar methodisch auf diese Instrumente, insbesondere auf das Risiko- und Kontinuitätsmanagement, ihn mit diesen gleichzusetzen wäre aber falsch.

2.3 Rollen und Zusammenarbeit

Die Umsetzung des SKI-Leitfadens erfordert eine enge Zusammenarbeit zwischen den Betreibern und den zuständigen Fachbehörden auf den Ebenen Bund, Kantone und ggf. Gemeinden. Eine wichtige Bedeutung können aber auch die verschiedenen Branchenverbände einnehmen. Folgende Rollen und Funktionen sind grundsätzlich möglich:

Rolle	Funktion
KI-Betreiber	➢ Federführung bei der Umsetzung des Leitfadens ➢ Einbringen des Unternehmenswissens ➢ Umsetzung der Massnahmen im KI-Betrieb
Branchenverbände	➢ Koordination bzw. Interessensvertretung der Betreiber ➢ Evtl. Mitarbeit bei der Erarbeitung von Branchenlösungen
Behörden	➢ Empfehlung an die KI-Betreiber zur Anwendung des SKI-Leitfadens ➢ Begleitung / Abstützung des Prozesses auf politisch-gesellschaft-licher Ebene ➢ Regelung der Umsetzung und Finanzierung von allenfalls zusätzlich notwendigen Massnahmen

Tabelle 2: Rollen und Funktionen

Eine Zusammenarbeit mit den Behörden und ein gegenseitiger Austausch innerhalb und mit artverwandten Branchen sind aus folgenden Gründen angezeigt:

- In der Regel sind in den verschiedenen kritischen Teilsektoren jeweils mehrere Betreiber vom SKI-Leitfaden angesprochen. Entsprechende Branchenverbände erleichtern die Koordination bzw. Interessensvertretung gegenüber den zuständigen Fach-, Aufsichts- und Regulationsbehörden. Zudem kann sich die Möglichkeit anbieten, allenfalls zusätzlich notwendige Massnahmen im Rahmen von Branchenlösungen zu regeln (z. B. in Form einer verbesserten Zusammenarbeit bzw. gegenseitigen Hilfestellung im Ereignisfall). Damit kann der Aufwand für die einzelnen Unternehmen reduziert werden (sowohl bei der Umsetzung des Leitfadens als auch in Bezug auf allfällige zusätzliche Massnahmen).
- Geeignete Schutzmassnahmen für kritische Infrastrukturen können rasch den betrieblichen bzw. den betriebswirtschaftlichen Rahmen eines KI-Betreibers sprengen. Mit einem Einbezug von Branchenverbänden und den zuständigen Fachbehörden wird sichergestellt, dass die Finanzierung im Rahmen des jeweiligen Politikbereiches (z. B. Energiepolitik, Verkehrspolitik usw.) sichergestellt werden kann.

3 Integraler Schutz von kritischen Infrastrukturen

Die Vorgehensweise beim integralen Schutz von kritischen Infrastrukturen basiert auf einem systematischen und kontinuierlichen Prozess (siehe Abbildung 2):

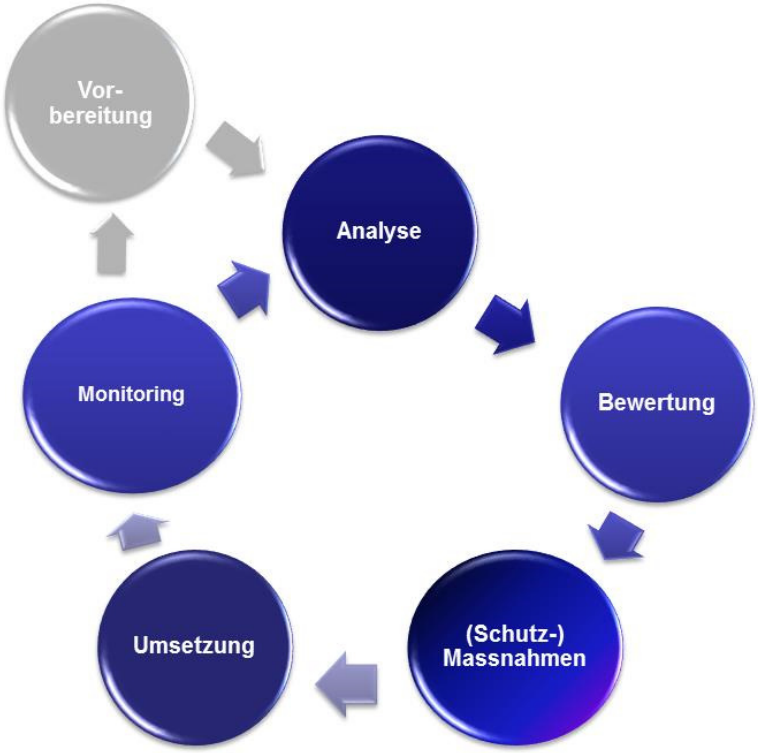


Abbildung 2: Prozess zum integralen Schutz von kritischen Infrastrukturen

Nach einer Phase der Vorbereitung, in welcher Zuständigkeiten geklärt, Kompetenzen verteilt und Aufträge eingeholt werden, erfolgt der iterative Prozess zur Verbesserung des Schutzes kritischer Infrastrukturen in fünf Phasen:

In der Phase 1, der Analyse, werden kritische Prozesse identifiziert und Gefährdungen analysiert, die zu einem Ausfall dieser Prozesse führen können. Anschliessend werden die daraus entstehenden Risiken ermittelt und miteinander verglichen.

In Phase 2 erfolgt die Bewertung der Risiken und Verwundbarkeiten.

Während Phase 3 werden Massnahmen evaluiert, mit denen die Risiken wirksam reduziert werden können.

Phase 4 beinhaltet die Umsetzung der Massnahmen. Dabei wird aufgezeigt, wie die Massnahmen geplant, umgesetzt, begleitet und überwacht werden können.

Phase 5 behandelt das Monitoring, die Überprüfung und Verbesserung der Massnahmen. Damit sollen der Umsetzungsfortschritt und die Wirksamkeit der Massnahmen kontinuierlich beobachtet werden.

3.1 Vorbereitung

Eine gründliche Vorbereitung schafft die Voraussetzungen für eine erfolgreiche Anwendung des Leitfadens SKI. Im Vorfeld sollten grundsätzliche Fragen geklärt werden. Hierzu zählen insbesondere die Auftragserteilung, die Zusammenstellung und Organisation einer Arbeitsgruppe, die Festlegung von Zuständigkeiten und die Bereitstellung von Ressourcen für diese Arbeiten.

3.1.1 Unterstützung durch die Leitungsebene und Auftragserteilung

Aufgrund der Bedeutung und der weitreichenden Konsequenzen der zu treffenden Entscheidungen ist es wichtig, dass die Umsetzung des Leitfadens vom zuständigen leitenden Organ des Betriebs (Geschäftsleitung oder Verwaltungsrat etc.) unterstützt wird. Dieses ist verantwortlich dafür, dass alle Geschäftsbereiche zielgerichtet und ordnungsgemäss funktionieren und dass Risiken erkannt, reduziert und die Auswirkungen auf den Betrieb bei Eintreten eines Schadensereignisses minimiert werden.[7]

Selbst wenn einzelne Aufgaben im Rahmen der Umsetzung des Leitfadens an Personen oder Organisationseinheiten delegiert werden, die diesbezüglich in der Folge die Verantwortung tragen, ist die Gesamtverantwortung nicht delegierbar und muss beim zuständigen leitenden Organ verbleiben. Das zuständige leitende Organ muss dafür sorgen, dass ausreichende Ressourcen (Personal, Zeit, finanzielle Ressourcen) für die Umsetzung des Leitfadens bereitgestellt werden.

Das zuständige leitende Organ hat für einen klaren Auftrag zur Umsetzung des Leitfadens zu sorgen. Darin sollten folgende Punkte geklärt werden:

- den Stellenwert des Vorhabens für den KI-Betreiber
- die Zielsetzung des Vorhabens
- der Geltungsbereich des Vorhabens
- die Struktur der Arbeitsgruppe zur Durchführung des Vorhabens mit den wichtigsten Rollen und deren Zuständigkeiten
- die zur Verfügung stehenden Ressourcen (Zeit, Personal, finanzielle Mittel etc.)

3.1.2 Erfassung von bestehenden Arbeiten

Im breiten Kontext des Schutzes kritischer Infrastrukturen existiert in der Regel eine Vielzahl von Arbeiten, die einzelne Aspekte von SKI behandeln. Die Umsetzung des SKI-Leitfadens baut stark auf diesen bestehenden Arbeiten und Planungen auf. Beispiele für möglicherweise bestehende Arbeiten sind:

Intern:

- Arbeiten in den Bereichen Risiko-, Notfall-, Krisen- und Kontinuitätsmanagement
- Implementierte Managementsysteme inkl. Prozesslandschaft
- Implementierte Führungsinstrumente und -tools
- Interne Vorschriften, Weisungen, Standards

Extern:

- Gesetzliche Grundlagen und Vorschriften
- Branchenstandards und Branchenlösungen
- Normen, Richtlinien und Leitfäden zu deren Umsetzung
- Nationale SKI-Strategie, SKI-Inventar und in diesem Kontext erarbeitete Funktionsstrukturen (enthält u. a. Angaben über kritische Prozesse und Elemente)

[7] Siehe dazu auch Artikel 55 des Schweizerischen Obligationenrechts.

- Teilsektorspezifische Berichte und Studien in Bezug auf die Verhinderung von Ausfällen bzw. die Reduktion von Schäden bei Ausfällen

3.2 Analyse

Im Rahmen der Analyse-Phase werden die kritischen Prozesse bezeichnet, relevante Gefährdungen und Verwundbarkeiten identifiziert sowie die entsprechenden Risiken ermittelt.

Folgendes Schema soll die einzelnen Schritte innerhalb dieses Kapitels verdeutlichen:

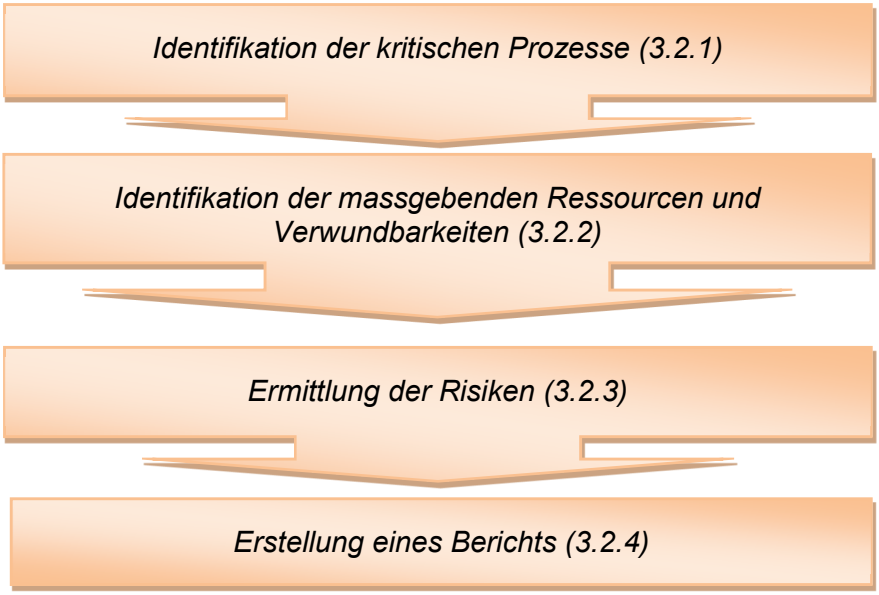


Abbildung 3: Ablaufschema Analyseschritte

3.2.1 Identifikation der kritischen Prozesse

Voraussetzung für den umfassenden Schutz einer kritischen Infrastruktur sind ausführliche Kenntnisse über deren Aufgaben und Funktionen. Darum muss verstanden werden, welche Prozesse unbedingt erforderlich sind, um ein Mindestmass an Funktionsfähigkeit der kritischen Infrastruktur zu gewährleisten.

Die Identifikation der kritischen Prozesse basiert massgeblich auf der umfassenden Analyse der betriebsrelevanten Prozesse im Rahmen des betrieblichen Kontinuitätsmanagements (Business Impact Analyse). Falls dies noch nicht erfolgt ist, geben die entsprechenden Normen und Richtlinien (vgl. Tabelle 1) Auskunft über das Vorgehen.

*Im Rahmen des Schutzes kritischer Infrastrukturen wird unter einem **kritischen Prozess** ein Prozess verstanden, welcher für die Funktionsfähigkeit der kritischen Infrastruktur existentiell wichtig ist und bei dessen Ausfall die Bevölkerung und deren Lebensgrundlagen unmittelbar in einem schweren Masse betroffen sein könnten.*

Dabei sollte auf eine handhabbare Anzahl identifizierter kritischer Prozesse geachtet werden. Nachfolgende Tabelle 3 gibt einen Überblick über ein **fiktives** Beispiel von kritischen Prozessen:

Nr.	Kritischer Prozess
1	Produktion
2	Systemführung und -steuerung
3	Distribution

Tabelle 3: Beispiele für kritische Prozesse

3.2.2 Identifikation der massgebenden Ressourcen und Verwundbarkeiten

Als Nächstes ist zu beurteilen, welche Ressourcen zur Durchführung der zuvor als kritisch identifizierten Prozesse zwingend erforderlich sind. Dabei sind insbesondere die Ressourcenbereiche Rohstoffe, Energie, IKT, Arbeitskräfte sowie Logistik und Infrastruktur zu berücksichtigen.

Nachfolgende Abbildung 4 dient zur Illustration des Vorgehens:

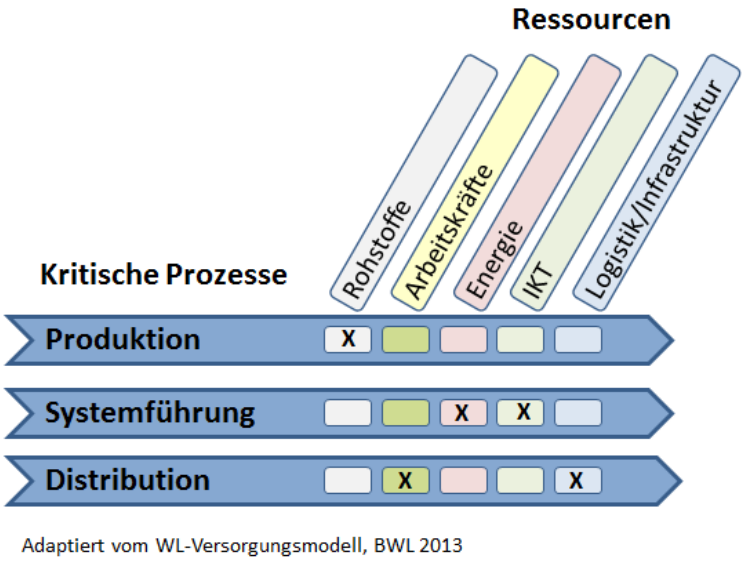


Abbildung 4: Prozess- und Ressourcenmodell

In der Folge ist zu beschreiben, welche Auswirkungen ein Ausfall der jeweiligen Ressource in Bezug auf den kritischen Prozess nach sich ziehen respektive inwieweit ein Ausfall der Ressource die Durchführung des Prozesses beeinträchtigen würde.

3.2.3 Ermittlung der Risiken

Anschliessend gilt es zu ermitteln, welche Risiken für die Bevölkerung und ihre Lebensgrundlagen die in Schritt 3.2.3 aufgezeigten Verwundbarkeiten darstellen.

*Das **Risiko** ist ein Mass für die Grösse einer Gefährdung. Es kann als Produkt der Eintrittswahrscheinlichkeit respektive Plausibilität eines Ereignisses und des daraus an der Bevölkerung und ihren Lebensgrundlagen resultierenden Schadensausmasses dargestellt werden.*

Der Begriff Risiko dient beim Schutz kritischer Infrastrukturen sowohl als Modell zur Beurteilung von Sicherheitsfragen als auch dazu, verschiedene Gefährdungen anhand gleicher Kriterien miteinander vergleichen zu können.

Die beiden zentralen Faktoren des Risikos sind somit die Eintrittswahrscheinlichkeit sowie das Schadensausmass eines Ereignisses.

*Als **Eintrittswahrscheinlichkeit** wird das geschätzte bzw. auf Statistikwerten beruhende Eintreten eines Ereignisses innerhalb einer bestimmten Zeitspanne bezeichnet.*

*Als **Schadensausmass** werden die geschätzten Auswirkungen auf die Bevölkerung und deren Lebensgrundlagen bezeichnet, die durch den Ausfall eines oder mehrerer kritischer Prozesse bei Eintritt der Gefährdung entstehen. Das Schadensausmass besteht aus der Summe des Schadens zum Zeitpunkt des Eintritts eines Ereignisses und des Schadens, der während der ganzen Wiederherstellungszeit entstehen kann.*

Die Ermittlung der Risiken erfolgt in drei Schritten: Zunächst werden die relevanten Gefährdungen identifiziert. Anschliessend werden entsprechende Szenarien erarbeitet, die schliesslich bezüglich ihrer Eintrittswahrscheinlichkeit bzw. Plausibilität sowie des Schadensausmasses für die Bevölkerung und ihrer Lebensgrundlage eingeschätzt werden.

Schritt 1: Auswahl der relevanten Gefährdungen

Die in Kapitel 3.2.1 und 3.2.2 als massgebend bestimmten Prozesse und Ressourcen sind in einer Tabelle aufzulisten und mit einer eindeutigen Nummer zu versehen. Für diejenigen Ressourcen, die sich im **eigenen Verantwortungsbereich** befinden, sind anschliessend **relevante** Gefährdungen auszuwählen, die zu einem Ausfall der Ressource führen können.[8] Dabei ist ein umfassendes Gefahrenspektrum zu berücksichtigen, d. h. es sind grundsätzlich alle potenziell möglichen Gefährdungen zu berücksichtigen, die zu einem signifikanten Ausfall der Ressource führen können. Als Hilfsmittel zur Identifikation steht unter anderem ein Gefährdungskatalog des BABS zur Verfügung.[9]

- Gefährdungskatalog: Der Gefährdungskatalog stellt eine umfassende und bei Bedarf anpassbare Zusammenstellung von Ereignissen und Entwicklungen dar, welche die Bevölkerung und ihre Lebensgrundlagen heute und künftig gefährden können. Der Gefährdungskatalog gibt eine möglichst vollständige Übersicht über denkbare Ereignisse und Entwicklungen, ohne diese zu priorisieren. Der Katalog ist ressourcenspezifisch mit weiteren Gefährdungen, die zu Ausfällen führen können, zu ergänzen.

[8] Dabei handelt es sich um Ressourcen, bei denen mittels präventiven Massnahmen verhindert werden kann, dass es zu einem Ausfall der Ressource kommt. Es besteht also ein Unterschied zu den vorsorglichen Massnahmen, die verhindern, dass der Ausfall der Ressource zu einem Ausfall des Prozesses führt.

[9] www.risk-ch.ch -> Gefährdungskatalog

Für externe Ressourcen (externe Leistungserbringer, Dienstleistungen usw.) ist jeweils der Ausfall der entsprechenden Ressource zu untersuchen, unabhängig von der jeweiligen Ursache. Tabelle 4 zeigt ein fiktives Beispiel für eine entsprechende Zusammenstellung.

Nr.	Kritische Prozesse gemäss Kap. 3.2.1	Massgebende Ressourcen gemäss Kap. 3.2.2	Ausfall externer Ressourcen / relevante Gefährdung für Ressourcen im eigenen Verantwortungsbereich
1	Produktion	*Rohstoffe (extern)*	*Ausfall Rohstoff*
2	Produktion	Bauten / Anlagen (Fabrik X)	Erdbeben
3	Produktion	Bauten / Anlagen (Fabrik X)	Konventioneller Anschlag
3	Systemführung und -steuerung	*IKT (extern)*	*Ausfall öffentliche Telekommunikation*
4	Systemführung und -steuerung	IKT (Firmennetzwerk)	Cyber-Angriff
5	Systemführung und -steuerung	Personal (Systemführer)	Pandemie
7	Distribution	*Energie (extern)*	*Ausfall Stromversorgung*
8	Distribution	Bauten / Anlagen (Verteilzentrale Z)	Brand

Tabelle 4: Beispiel für eine Gegenüberstellung von Prozessen, Ressourcen und Gefährdungen

Schritt 2: Erarbeitung der Szenarien

In einem nächsten Schritt sind Szenarien zu bilden, welche beispielhaft beschreiben, in welcher Form und in welcher Ausprägung die jeweils massgebende Ressource ausfällt bzw. wie die relevante Gefährdung die Ressource beeinträchtigt und welche Konsequenzen dies für die Bevölkerung und ihre Lebensgrundlagen hat. Beispiele für Szenarien und Informationen zu verschiedenen Gefährdungen bieten u. a. die Arbeiten zur nationalen Gefährdungsanalyse «Katastrophen und Notlagen Schweiz».[10]

Da beim Schutz kritischer Infrastrukturen davon ausgegangen wird, dass Alltagsereignisse und deren Auswirkungen von den Betreibern beherrscht werden und für die Gemeinschaft keine Probleme darstellen, stehen jeweils Ereignisse mit einer grossen bis extremen Intensität im Vordergrund. Die Arbeiten sollen sich zudem am Prinzip des *credible worst case* orientieren. Das heisst, dass jeweils davon auszugehen ist, dass die Gefährdung in einer denkbar ungünstigen Ausprägung auf die jeweilige Ressource einwirkt.[11] Für die maximale Ausfallzeit von Anlagen sind realistische Annahmen zu treffen bzgl. Reparaturdauer bzw. bis zur Einsatzbereitschaft alternativer Versorgungsmöglichkeiten. Dabei sind die Rahmenbedingungen der untersuchten Gefährdung mit zu berücksichtigen (z. B. wenn ein entsprechendes Ereignis zu grossflächigen Schäden führt und dadurch die Verfügbarkeit von Ersatzteilen oder Fachpersonal reduziert ist).

[10] www.risk-ch.ch

[11] Beispielsweise ist in Bezug auf die Ressource Bauten und Anlagenund die Gefährdung Erdbeben im Falle von zwei redundanten Standorten (z. B. Rechenzentren) ein Erdbeben zu betrachten, das mit grösstmöglicher Intensität auf beide Standorte gleichzeitig einwirkt.

Schritt 3: Einschätzung der Szenarien

In Bezug auf die beschriebenen Szenarien sind nun die möglichen Schadensauswirkungen zu ermitteln. Im Gegensatz zu herkömmlichen Risiko- und Kontinuitätsmanagement-Ansätzen stehen dabei nicht die Auswirkungen *für das Unternehmen* im Vordergrund, sondern jene *auf die Bevölkerung und ihre Lebensgrundlagen*.

Damit dieses Schadensausmass ermittelt werden kann, müssen geeignete Indikatoren festgelegt werden. Nachfolgend wird ein Vorschlag für Indikatoren zur Bestimmung der Schäden an der Bevölkerung und ihren Lebensgrundlagen gemacht, die infolge von Ausfällen oder Störungen der kritischen Infrastrukturen entstehen können. Dabei ist es durchaus möglich, dass je nach kritischer Infrastruktur einzelne Indikatoren nicht berücksichtigt oder zusätzliche Indikatoren festgelegt werden. Die Auswahl ist im Rahmen der Berichterstattung zu dokumentieren und zu begründen.

Schadensbereich	Teilbereich	Indikator	Abstützung in Bundesverfassung	Masseinheit
Personen	Leben und Gesundheit	**Todesopfer**	Art. 10, 57, 58, 61,118	Anzahl
		Verletzte/Kranke		Anzahl
	Hilfe in Notlagen	**Unterstützungsbedürftige**	Art. 12, 115	Personen x Tage
Umwelt	Ökosystem	**Geschädigte Ökosysteme**	Art. 74, 76, 77, 78, 104	Fläche x Jahre
Wirtschaft	Vermögen	**Vermögensschäden und Bewältigungskosten (Sachvermögen, Finanzvermögen)**	Art. 61	CHF
	Wirtschaftliche Leistungsfähigkeit	**Reduktion der wirtschaftlichen Leistungsfähigkeit**	Art. 100	CHF
Gesellschaft	Versorgung mit lebensnotwendigen Gütern und Dienstleistungen	**Beeinträchtigung der Lebensqualität**	Art. 102	Personen x Tage
	Verfassungsmässige Ordnung, innere Sicherheit	**Einschränkungen von Ordnung und innerer Sicherheit**	Art. 52, 185	Personen x Tage
	Ansehen und Vertrauen in den Staat	**Geschädigtes Ansehen**	Art. 54	Intensität x Dauer
		Vertrauensverlust in Staat/Institutionen	Präambel, Art. 2, 5	Intensität x Dauer
	Territoriale Integrität	**Einschränkung der territorialen Integrität**	Art. 58	Intensität x Dauer
	Kulturgüter	**Schädigung und Verlust von Kulturgütern**	Art. 2, 69, (78)	Anzahl x Bedeutung

Tabelle 5: Vorschlag für mögliche Schadensindikatoren

Detaillierte Angaben zu den einzelnen Schadensindikatoren und Vorschläge für entsprechende Klassen sind im Anhang 2 – Schadensindikatoren zu finden.

W I C H T I G !

Bei der Ermittlung des Schadensausmasses stehen die Schäden an der Bevölkerung und ihren Lebensgrundlagen im Vordergrund, die durch den Ausfall, die Störung oder Zerstörung der kritischen Infrastruktur verursacht werden. Insbesondere sind die (vielfach schwierig zu quantifizierenden) indirekten Folgeschäden zu berücksichtigen, die sich durch den Ausfall der kritischen Prozesse bis zu deren Instandstellung ergeben. Unter anderem ist dabei von Bedeutung, ob ausreichende Redundanzen vorhanden sind bzw. ob alternative Möglichkeiten bestehen, die Leistung zu überbrücken (z. B. Strassenverkehr statt Schienenverkehr).

Nach der Ermittlung des Schadensausmasses ist die Eintrittswahrscheinlichkeit bzw. die Plausibilität der Szenarien zu beurteilen. Dazu sind zunächst geeignete Indikatoren bzw. Klassen zu definieren. Anhang 3 enthält einen Vorschlag für entsprechende Indikatoren und Klassen.[12] Die Festlegung der Indikatoren zur Bestimmung der Eintrittswahrscheinlichkeit ist im Rahmen der Berichterstattung ebenfalls zu dokumentieren und zu begründen. Mit Hilfe dieser Indikatoren wird anschliessend die Wahrscheinlichkeit oder Plausibilität für das jeweilige Szenario bewertet.[13]

Die Werte bezüglich Schadensausmass und Eintrittswahrscheinlichkeit werden anschliessend in die Zusammenstellung der kritischen Prozesse und der Gefährdungen eingetragen. In Bezug auf die verschiedenen Indikatoren zur Beurteilung des Schadensausmasses wird empfohlen, den Wert der höchsten Ausmassklasse anzugeben.

Nr.	Kritischer Prozess gemäss Kap. 3.2.1	Massgebende Ressource gemäss Kap. 3.2.2	Relevanter Ressourcenausfall bzw. Gefährdung für Ressourcen im eigenen Verantwortungsbereich	Risiko
1	Produktion	*Rohstoffe (extern)*	*Ausfall Rohstoff*	A3 / W3
2	Produktion	Bauten / Anlagen (Fabrik X)	Erdbeben	A5 / W5
3	Produktion	Bauten / Anlagen (Fabrik X)	Konventioneller Anschlag	A6 / W2
4	…	…	…	…
5	…	…	…	…

Tabelle 6: Ergänzung der beispielhaften Gegenüberstellung von kritischen Prozessen, Ressourcen und Gefährdungen (Tabelle 4) mit Wahrscheinlichkeit und Schadensausmass

Die entsprechenden Werte können schliesslich in einer Risikomatrix grafisch dargestellt werden. Dadurch lassen sich die verschiedenen Risiken auf einen Blick erfassen. Abbildung 5 zeigt ein Wahrscheinlichkeits-Risiko-Diagramm für die Prozesse 1–3 (alternativ oder ergänzend dazu kann auf der Vertikalachse die Plausibilität aufgetragen werden).

[12] Für weiterführende Angaben zur KNS-Methode vgl. Methode zur Risikoanalyse von Katastrophen und Notlagen für die Schweiz, Version 1.03

[13] Das BABS stellt Grundlagen zur Bewertung der Plausibilität bzw. Eintrittswahrscheinlichkeit sowie zur Ausprägung der Szenarien zur Verfügung.

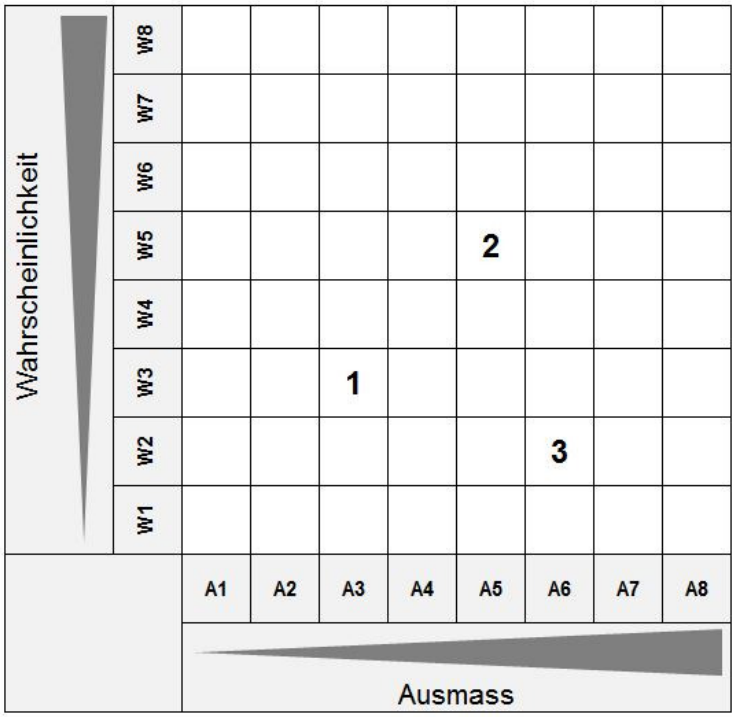


Abbildung 5: Beispiel einer Risikomatrix

3.2.4 Erstellung eines Analyse-Berichts

Der Analyse-Bericht sollte alle wesentlichen Informationen, die in den Phasen Vorbereitung und Analyse erhoben wurden, enthalten. Die Aufnahme des Ist-Zustandes ist auf die kritischen Prozesse zu beschränken.

Sollte die Analyse grosse Sicherheitslücken bei den kritischen Prozessen aufdecken (z. B. *Single Point of Failure*, Nichteinhaltung von gesetzlichen Auflagen etc.), so sind im Bericht auch gleich Massnahmen vorzuschlagen, die für die Schliessung dieser gravierenden Sicherheitslücken zeitnah umzusetzen sind.

Der Analyse-Bericht soll folgende Punkte abdecken:

- Kurze Systembeschreibung
- Angaben zu massgebenden bestehenden Vorarbeiten (RM- und BCM-Grundlagen)
- Angaben zu kritischen Prozessen
- Angaben zu massgebenden Ressourcen und Verwundbarkeiten
- Relevante Gefährdungen
  - Relevante Indikatoren für das Ausmass je Gefährdung inkl. kurze Begründung für nicht relevante Indikatoren
  - Ausmass und Wahrscheinlichkeit der Szenarien
  - Bereits realisierte Sicherheitsmassnahmen bzw. in der Analyse berücksichtigte, bereits geplante Massnahmen
- Risikomatrix
- Erkannte Lücken / erforderliche Sofortmassnahmen (wo bereits bekannt)

Der Analyse-Bericht wird im Verlauf der weiteren Arbeiten mit Ergebnissen zu den Phasen Bewertung und (Schutz-)Massnahmen zu einem Gesamtbericht ergänzt. Anhang 6 enthält einen Vorschlag für eine mögliche Gliederung. Der Analysebericht deckt Kapitel 1-3 des Gesamtberichts ab.

3.3 Bewertung

Im Anschluss an die Gefährdungs- und Verwundbarkeitsanalyse ist festzulegen, welches Niveau an Sicherheit angestrebt werden soll. Dies erfolgt im Rahmen der Phase Bewertung. Dabei sind insbesondere die strategischen Zielsetzungen relevant, die u.a. in der nationalen SKI-Strategie festgelegt wurden (vgl. dazu auch Kapitel 1.2)

In Bezug auf die Phase der Bewertung stehen insbesondere folgende Fragen im Vordergrund:

- *Wie sicher ist sicher genug?*
- *Was nehmen wir in Kauf, sollte ein Ereignis eintreten?*
- *Wie viel sind wir bereit zu investieren, um die Sicherheit zu erhöhen?*

Als Richtvorgabe dienen zunächst die strategischen Zielsetzungen in Bezug auf das anzustrebende Sicherheitsniveau.

Das Sicherheitsniveau bezeichnet den von allen Verantwortungsträgern gemeinsam angestrebten Sicherheitszustand.

In Anlehnung an die nationale SKI-Strategie wird in Bezug auf kritische Infrastrukturen folgendes Sicherheitsniveau angestrebt: *Die Schweiz ist im Hinblick auf kritische Infrastrukturen resilient, so dass grossflächige und schwerwiegende Ausfälle der kritischen Infrastrukturen möglichst verhindert werden beziehungsweise im Ereignisfall das Schadensausmass möglichst gering gehalten wird.*[14]

In Bezug auf Naturgefahren ist von der Nationalen Plattform Naturgefahren PLANAT zudem folgendes Sicherheitsniveau vorgegeben: «*Das Risiko [...] ist so gering, dass der Fortbestand der Gemeinschaft heute und über die nächsten Generationen gesichert ist. Lebenswichtige Güter und Dienstleistungen dürfen nur für kurze Zeit in grossen Teilen der Schweiz ausfallen.*»[15]

Mit Schutzzielen wird anschliessend der konkrete Beitrag der verschiedenen Verantwortungsträger zur Erreichung des Sicherheitsniveaus festgelegt.

Ein Schutzziel bezeichnet das Niveau an Sicherheit, das bestimmte Verantwortungsträger in ihrem Verantwortungsbereich grundsätzlich anstreben.

In verschiedenen Bereichen des Schutzes kritischer Infrastrukturen (z. B. in einzelnen Teilsektoren oder in Bezug auf einzelne Gefährdungen) sind bereits Schutzziele vorgegeben. Diese sind im Rahmen der Arbeiten zur Umsetzung des SKI-Leitfadens zwingend zu berücksichtigen. Insbesondere sind Schutzziele in Bezug auf individuelle Risiken (z. B. Todesfallrisiko) einzuhalten.

Bei den kollektiven Risiken (vor allem dort, wo noch **keine** Schutzziele definiert sind), erfolgt eine Bewertung der Risiken und der zu ihren Minderung möglichen Massnahmen im Rahmen der Massnahmenplanung u. a. mittels des Grenzkosten-Ansatzes.[16] Die Grenzkosten stellen die Grenze der Zahlungsbereitschaft der Gesellschaft zur Verhinderung *einer* Schadenseinheit

[14] Nationale Strategie zum Schutz kritischer Infrastrukturen 2018-2022, BBl 2018 503.
[15] Nationale Plattform Naturgefahren PLANAT (2013): Sicherheitsniveau für Naturgefahren, August 2013, S. 11.
[16] Abhängig vom verfolgten Ansatz nehmen die Schutzziele eine andere Funktion ein: Im Bereich der Naturgefahren dienen die Schutzziele beispielsweis als Überprüfungskriterium zur Abklärung des Handlungsbedarfs. Handlungsbedarf besteht demnach insbesondere dann, wenn gewisse Grenzwerte in Bezug auf das Gesamtrisiko oder einzelne Faktoren des Risikos (Eintrittswahrscheinlichkeit oder Schadensaumsass) überschritten werden. Demgegenüber kennt der Grenzkosten-Ansatz, der in Ergänzung zu den bestehenden Ansätzen zur Anwendung kommt, keine solchen Grenzwerte in Bezug auf das Risiko. Der SKI-Leitfaden ist so gehalten, dass er mit beiden Ansätzen kompatibel ist.

dar (d. h. wie viel ist die Gemeinschaft bereit zu zahlen, um *ein* Todesopfer oder *einen* Franken wirtschaftlichen Schaden oder die Schädigung *einer* bestimmten Fläche Umwelt usw. zu verhindern?).

3.3.1 Vorgehen in Bezug auf die Bewertung der Risiken und Verwundbarkeiten

Das konkrete Vorgehen im Rahmen der Phase Bewertung erfolgt in Form von vier Schritten:

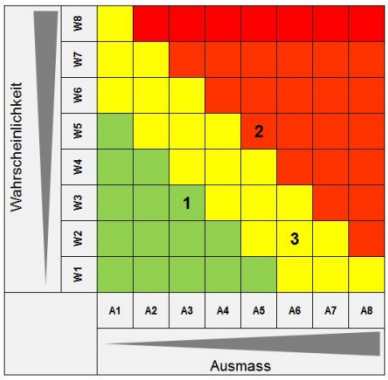
Schritt 1: Bewertung gegenüber bestehenden Vorgaben

Die Erfüllung der bestehenden rechtlichen Vorschriften (legal compliance) bildet den Ausgangspunkt. Diese Vorschriften umfassen alle Massnahmen, zu welchen ein KI-Betreiber aus rechtlichen Gründen verpflichtet ist (Einhaltung von gesetzlichen Vorgaben, Normen, best practices etc.). Weiter gehört auch die Erfüllung von anderweitig geltenden Schutzzielen dazu. Werden in Bezug auf die ermittelten Risiken die geltenden Vorschriften nicht eingehalten, sind umgehend Massnahmen zu deren Erfüllung zu treffen (gemäss Kapitel 3.4).

Schritt 2: Priorisierung der Risiken

Die Risikoanalyse kann bei Vorhandensein mehrerer Gefährdungsszenarien und kritischer Prozesse zu einer Grosszahl von Risikobeiträgen führen. Diese haben in der Regel unterschiedliche Bedeutung. Um die Quantifizierung der Risiken und die anschliessende Massnahmenplanung zu vereinfachen, können in einer ersten Phase die Risikobeiträge nach ihrer Grössenordnung triagiert bzw. provisorische Grenzwerte als Zielvorstellung formuliert werden.

Dazu werden die Risiken innerhalb der Risikomatrix drei Prioritätsstufen zugeteilt:



rot = prioritäre Massnahmenplanung
gelb = sekundäre Massnahmenplanung
grün = zurückgestellte Massnahmenplanung

Abbildung 6: Vorschlag für Einteilung der Prioritätsstufen

Dabei ist es auch möglich, zur Entlastung der Arbeiten einen Grenzbereich festzulegen, in denen auf eine anschliessende Risikoquantifizierung und Massnahmenplanung verzichtet werden kann. Die Festlegung des Grenzbereichs ist zu begründen und im abschliessend zu erstellenden Bericht festzuhalten.

Schritt 3: Festlegung der relevanten Grenzkosten und der Aversion

Damit eine Quantifizierung der Risiken erfolgen kann, müssen die verschiedenen Indikatoren zur Bestimmung des Schadensausmasses (vgl. Kapitel 3.2.3, Schritt 3) in eine Geldeinheit transformiert werden. Dabei gilt es festzulegen, wie viel die Gesellschaft zur Verhinderung einer Schadenseinheit zu zahlen bereit ist.

Ausgangspunkt ist dabei ein Leitindikator, für den die besten Grundlagen inkl. Konsens für eine Monetarisierung mittels Zahlungsbereitschaft bestehen. Dies sind in der Regel die Todesopfer, für welche heute umfassende Grundlagen für eine Monetarisierung vorliegen. An

diesem Leitindikator werden die anderen Indikatoren anschliessend geeicht.[17] Ein Vorschlag findet sich in *Anh 4.1 – Vorschläge für Grenzkosten*.

Um dem Umstand Rechnung zu tragen, dass die Gesellschaft Grossrisiken besonders zu vermeiden versucht, kann ein Aversionsfaktor festgelegt werden.[18] Ein Vorschlag für eine Aversionsfunktion findet sich in *Anh 4.2 – Vorschlag für Aversionsfaktor* .

Die Festlegung der Grenzkosten und des Aversionsfaktors erfolgt in Absprache mit den zuständigen Fachbehörden. Um die Vergleichbarkeit mit anderen Analysen zu gewährleisten, sind die Risiken sowohl mit als auch ohne Aversion zu betrachten.

Schritt 4: Quantifizierung der Risiken

Für die in der Risikomatrix als prioritär zu behandelnden identifizierten Risiken wird mit Hilfe der monetarisierten Schadensindikatoren und gegebenenfalls der Aversionsfunktion eine detaillierte, quantitative Risikoanalyse durchgeführt. Für die Weiterbearbeitung empfiehlt es sich, die Risiken auf jährliche Schadenserwartungswerte umzurechnen und pro Prozess respektive Gefährdung zu addieren. Damit ergibt sich eine Übersicht über die jährlichen Schadenserwartungswerte pro Prozess respektive pro Gefährdungsart (vgl. Abbildung 7). Zudem kann das für die kritischen Infrastrukturen resultierende Gesamtrisiko ermittelt werden (jährlicher Schadenserwartungswert).

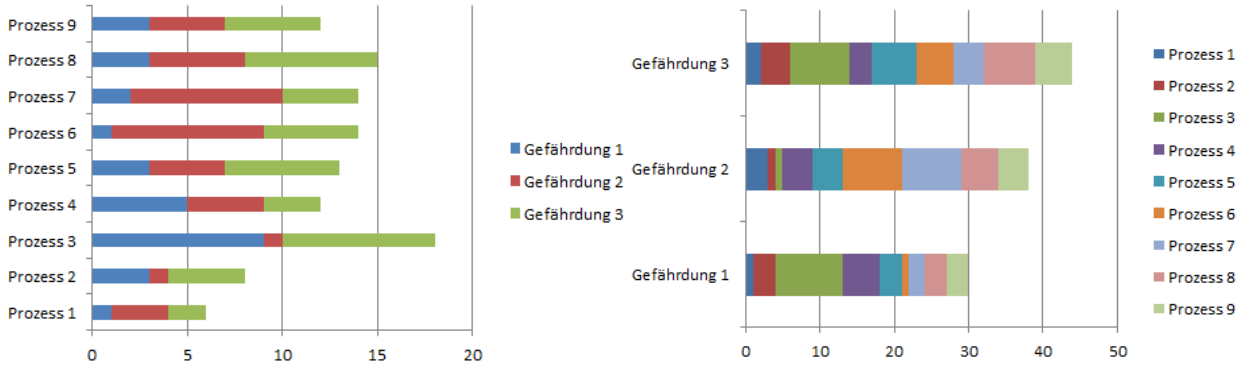


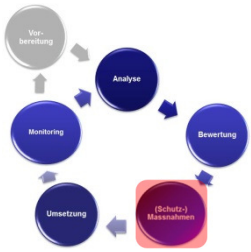
Abbildung 7: Übersicht und Struktur der Risiken für ein fiktives Beispiel mit 9 Prozessen und 3 Gefährdungsarten. Links: Risiken der Gefährdungen über alle Prozesse. Rechts: Risiken der Prozesse über alle Gefährdungen.

Die entsprechend monetarisierten Risiken bilden die Basis für die anschliessende Massnahmenplanung. Dabei gilt es zu überprüfen, mit welchen Massnahmen inklusive der damit verbundenen Kosten die Risiken auf ein akzeptables Niveau gesenkt werden können. Der endgültige Entscheid über die Realisierung der Massnahmen (und damit im Endeffekt auch über die konkret zu erreichende Sicherheit) erfolgt nach Ausarbeitung der optimalen Massnahmenkombination; wobei im Rahmen einer Güterabwägung auf politischer Ebene auch anderweitige Interessen zu berücksichtigen sind (vgl. Kapitel 3.4.4). Der nach der Analyse-Phase erstellte Bericht ist mit den Ergebnissen der Phase Bewertung zu ergänzen. Insbesondere ist zu dokumentieren, welche Grenzkosten zur Festlegung der Zahlungsbereitschaft für die verschiedenen Indikatoren gewählt wurden.

[17] Analog der Einteilung bei der nationalen Gefährdungsanalyse Katastrophen und Notlagen Schweiz, http://www.risk-ch.ch

[18] So wird z. B. ein Grossunfall im Strassenverkehr mit 20 Todesopfern von der Öffentlichkeit wesentlich anders beurteilt als 20 Einzel-Unfälle mit je 1 Toten, obwohl der Risikowert derselbe ist.

3.4 (Schutz-)Massnahmen



Bei der Erarbeitung der Massnahmenplanung sind Massnahmen zu evaluieren, die grundsätzlich in Frage kommen, um die zuvor identifizierten und analysierten Risiken zu reduzieren. Dabei stellen sich folgende grundlegenden Fragen:

- Wie können Auswirkungen minimiert werden?
- Wo bestehen Lücken (welche Schutzmassnahmen fehlen)?
- Welche bereits existierenden Schutzmassnahmen müssen ergänzt bzw. angepasst werden?
- Wie viel wollen wir für Massnahmen investieren, um die Sicherheit zu erhöhen?

Der Vorgang, mit welchem diese Fragen beantwortet werden, ist in den folgenden Unterkapiteln beschrieben.

Grundsätzlich stehen in Bezug auf die Bewältigung der identifizierten Risiken drei Optionen zur Auswahl: Risiken vermeiden, Risiken reduzieren und Risiken überwälzen. Da es sich bei kritischen Infrastrukturen um unverzichtbare Funktionen mit essenzieller Bedeutung für die Gesellschaft und die Wirtschaft handelt, deren Risiken weder vollständig vermeidbar sind noch adäquat versichert werden können, konzentrieren sich die nachfolgenden Ausführungen auf Aspekte bezüglich der Risikoreduktion.

3.4.1 Zusammentragen von möglichen Massnahmen

In einem ersten Schritt sind sämtliche möglichen Massnahmen zusammenzutragen, mit denen sich die Risiken reduzieren lassen. Dabei ist ein umfassendes Spektrum zu berücksichtigen, z. B.:

- Bauliche Massnahmen (passiv, Abschirmung der Gefahr)
- Technische Massnahmen (aktiv, «wenn …, dann …»)
- Personelle Massnahmen (Schutzkleidung etc.)
- Organisatorisch-administrative Massnahmen (Gebote und Verbote)
- Rechtliche Massnahmen (Verträge, Leistungsvereinbarungen, Zusammenarbeit im Katastrophenfall etc.)

Beispiele solcher Schutzmassnahmen sind in Anhang 5 – Beispiele für Schutzmassnahmen aufgelistet. Sie haben informativen Charakter und dienen als Ergänzung zu evtl. bereits bestehenden Schutzmassnahmen. Die Auflistung ist nicht abschliessend. Für jede kritische Infrastruktur muss jeweils geklärt werden, welche Schutzmassnahmen bereits bestehen oder geplant sind.

Da gewisse Massnahmen durchaus kostenintensiv ausfallen können, wird empfohlen, bei der Massnahmenerarbeitung die Zusammenarbeit mit weiteren involvierten Stellen zu suchen. So kann es beispielsweise sinnvoll sein, Massnahmen in Form von Branchenlösungen zu treffen (z. B. verstärkte Zusammenarbeit im Ereignisfall, Beschaffung von gemeinsamen Ersatzmaterial usw.).

Weiter ist zu beachten, dass es unter Umständen bei einzelnen Gefährdungen mit extremer Intensität nicht sinnvoll oder möglich ist, diesen ausschliesslich mit Massnahmen an den kritischen Infrastrukturen selbst zu begegnen (z. B. mit Objektschutzmassnahmen). In solchen Fällen ist mit den gefährdungs- bzw. massnahmenspezifischen Fachstellen (z. B. Naturgefahren- oder Bevölkerungsschutzämter) zu prüfen, ob Massnahmen der öffentlichen Hand an der Gefahrenquelle bzw. bei der Gefahrenabwehr möglich sind.

Die nachfolgend beschriebenen Schritte bezüglich Massnahmenplanung und –umsetzung beziehen sich ausschliesslich auf Massnahmen zur Stärkung der Resilienz der kritischen Infrastrukturen an und für sich.

In Bezug auf Massnahmen zur Stärkung der Resilienz der kritischen Infrastrukturen stehen sowohl präventive als auch vorsorgliche Massnahmen zur Auswahl. Im Rahmen der Massnahmenplanung sind beide Bereiche zu berücksichtigen.

- **Präventive Massnahmen**

  Massnahmen, mit denen primär die Verletzlichkeit einer kritischen Infrastruktur verringert werden kann; d. h. Gefährdungen entstehen gar nicht erst oder sie können sich nur begrenzt auswirken. Massnahmen der Prävention entfalten ihre Wirkung vor der Entstehung eines Ereignisses.

- **Vorsorgliche Massnahmen**

  Massnahmen, die die Ausfallzeit einer kritischen Infrastruktur minimieren oder die Ereignisbewältigung unterstützen, um das Schadensausmass im Ereignisfall möglichst kleinzuhalten. Massnahmen der Vorsorge entfalten ihre Wirkung während oder nach Eintritt eines Ereignisses.

  Dabei sind insbesondere Massnahmen zur Sicherstellung der Kontinuität, zur Notfall- und zur Krisenbewältigung zu treffen respektive die entsprechenden Arbeiten in Bezug auf die in Kapitel 3.2 und 3.3 ermittelten Ergebnisse zu ergänzen.

  Grundlagen für solche Massnahmen sind in der nachfolgenden Zusammenstellung festgehalten:

Massnahmen	Erläuterungen
Massnahmen zur Sicherstellung der Kontinuität	Im Rahmen des Schutzes kritischer Infrastrukturen ist die Sicherstellung der Funktionsfähigkeit der kritischen Infrastrukturelemente in bestehenden *Business Continuity Management-Systemen* (BCM-Systeme) angemessen zu integrieren. Gegebenenfalls ist dafür eine Anpassung des BCM vorzunehmen. Sollten keine betriebsinternen Massnahmen zur Sicherstellung der Kontinuität existieren, sind solche im Rahmen eines BCM zu planen und zu dokumentieren. *Anleitungen und Hinweise für Massnahmen zur Sicherstellung der Kontinuität geben z. B.:* *- ISO 22301: Societal Security – Business Continuity Management Systems – Requirements* *- ISO 22313: Societal Security – Business Continuity Management Systems – Guidance. First edition, 15. December 2012.* *- BSI-Standard 100-4 Notfallmanagement, Version 1.0, 2008 (Fokus auf IT-Service Continuity Management)* *- Umsetzungsrahmenwerk zum Notfallmanagement nach BSI-Standard 100-4, 2013 (Fokus auf IT-Service Continuity Management)* *- BS 25999-2* *- BCI Good Practice Guidelines 2013* *- BCM-Ratgeber des Bundesamts für wirtschaftliche Landesversorgung («Unternehmenserfolg nachhaltig sichern – auch im Krisenfall»)* *- HB 221/2004 Business Continuity Management (basiert auf AS/NZS)*
Massnahmen zur Notfallbewältigung	Im Rahmen des Schutzes kritischer Infrastrukturen sind diese im bestehenden betriebsinternen Notfallmanagement angemessen zu integrieren. Die betriebsinternen Konzepte zur Alarmierung, Warnung und Evakuierung sind auf kritische Infrastrukturen zu übertragen. Im betriebsinternen Notfallmanagement sind für kritische Infrastrukturen die Sofortmassnahmen für Notfälle zu planen, vorzubereiten und ggf. anzupassen. Die Notfallorganisationen sind mit dem Notfallmanagement der kritischen Infrastrukturen vertraut zu machen. Die Sofortmassnahmen bei kritischen Infrastrukturen sind zu üben. Wenn kein betriebsinternes Notfallmanagement existiert, ist ein solches aufzubauen. *Anleitungen und Hinweise zum Aufbau eines Notfallmanagements geben z. B.:* *- BSI Standard 100-4* *- ISO / PAS 22399*

Massnahmen zur Krisenbewältigung	Im Rahmen des Schutzes kritischer Infrastrukturen sind diese im bestehenden betriebsinternen Krisenmanagement angemessen zu integrieren. Das Krisenmanagement ist so aufzubauen bzw. anzupassen, dass bei Ereignissen, welche die Funktionsfähigkeit einer kritischen Infrastruktur betreffen, immer der Krisenstab zum Einsatz kommt. Sollte kein betriebsinternes Krisenmanagement existieren, ist ein solches aufzubauen. *Anleitungen und Hinweise zur Bewältigung von Krisen bietet z. B.:* *- Führungsbehelf für Angehörige von zivilen Führungsorganen (Hrsg. Bundesamt für Bevölkerungsschutz BABS)* *Hinweise zum Aufbau eines Krisenmanagements finden sich u. a. in:* *- British Standards Institute – PAS 200:2011 – Crisis management. Guidance and good practice* *- «Präventive Schadenbewältigung: Mehr gewinnen als verlieren», Schweizerische Rückversicherungsgesellschaft Swiss Re, 2001.* *- ISO 22320: Sicherheit und Schutz des Gemeinwesens – Management der Gefahrenabwehr – Anforderungen an die Führungsstrukturen, 2011.*

Tabelle 7: Massnahmenbereiche mit Hinweisen auf Hilfsmittel und Literatur

3.4.2 Ermittlung der ökonomisch optimalen Massnahmenkombination

In einem nächsten Schritt geht es darum, aus den zusammengetragenen Massnahmen diejenigen zu bestimmen, die die ökonomisch optimale Massnahmenkombination bilden.

Ziel ist es dabei, ein optimales Verhältnis zu erreichen zwischen Schäden, die aus Ausfällen oder Störungen der KI resultieren, und den Kosten, die für die umzusetzenden Massnahmen aufzuwenden sind. Die optimale Massnahmenkombination liegt dort, wo die Gesamtkosten am tiefsten sind.

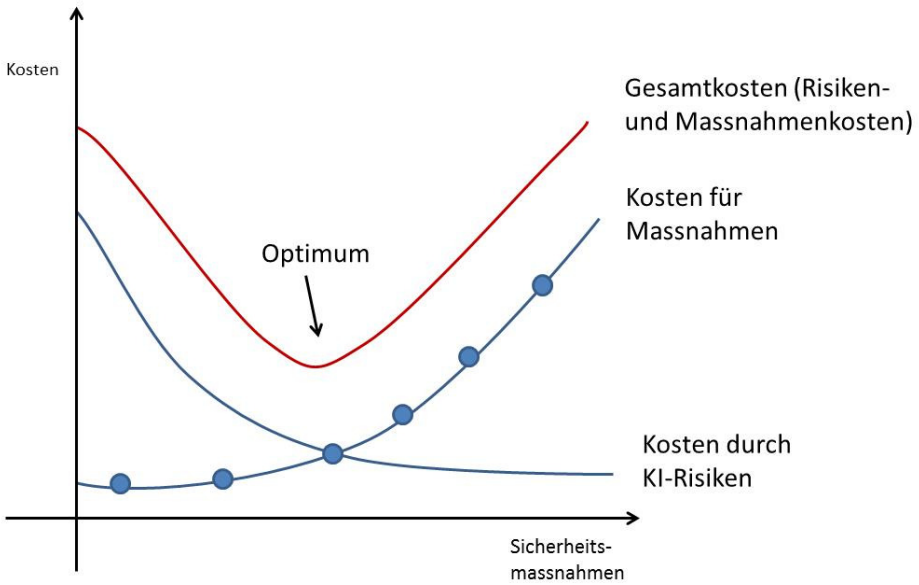


Abbildung 8: Prinzip der Grenzkosten: Die blauen Punkte stellen einzelne Massnahmen dar. Mit jeder implementierten Massnahme reduzieren sich die durch den Ausfall oder die Störung der KI zu erwartenden Schäden. Die optimale Massnahmenkombination liegt dort, wo die Gesamtkosten (d. h. die Kosten für Massnahmen und die Kosten für die Schäden, die aus Ausfällen oder Störungen der KI resultieren) am tiefsten sind.

Zu diesem Zweck werden aus der Liste sämtlicher möglicher Massnahmen diejenigen priorisiert, die vermutlich ein positives Kosten-Nutzen-Verhältnis aufweisen. Von diesen werden detailliert die jährlichen Kosten (Investitionskosten sowie wiederkehrende Kosten) ermittelt. Zudem wird geschätzt, um welchen Betrag die Risiken mithilfe dieser Massnahmen reduziert werden können. Anschliessend werden sämtliche risikoreduzierenden Massnahmen in ihrem Verhältnis von Risikoreduktion zu Massnahmenkosten absteigend aufgelistet und in einem

Diagramm mit den Massnahmenkosten entlang der Abszisse und der Risikoreduktion entlang der Ordinate zu einem Polygon aneinandergereiht (vgl. Abbildung 9). An dieses Polygon wird nun eine Gerade mit der Neigung -1 (Grenzkostenkriterium) herangeführt. Im Berührungspunkt ist das Grenzkostenkriterium gerade noch erfüllt. Rechts von diesem Punkt übertreffen die Kosten für die Schutzmassnahmen die Kosten der potenziellen Schadensreduktion. Links davon kostet jede Massnahme weniger als der Schaden, der mit der Massnahme verhütet werden kann.

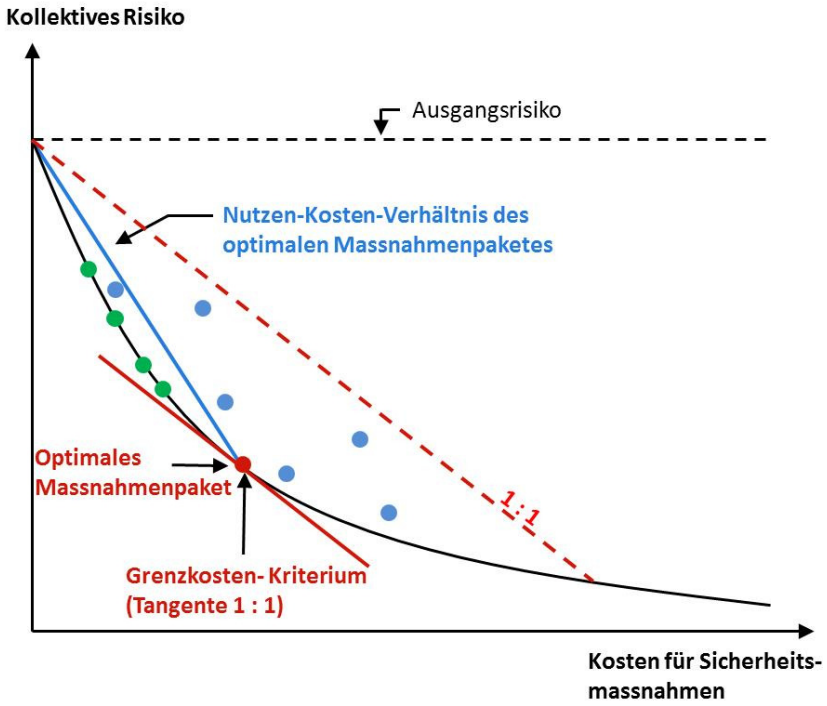


Abbildung 9: Vorgehen zur Ermittlung der ökonomisch optimalen Massnahmenkombination. Die schwarze Kurve ist die untere Begrenzung sämtlicher Massnahmen. Auf ihr erzielen Massnahmen bei minimalen Kosten ein Maximum an Nutzen (=Risikoreduktion). Alle Massnahmen unterhalb der rot gestrichelten Linie (blaue Punkte) weisen zwar ein Nutzen-Kosten-Verhältnis über 1 auf, sind aber nur effizient bzw. optimal, wenn sie auf der schwarzen Kurve bis zum roten Tangentenpunkt =Grenzkosten für Massnahmen liegen (grüne Punkte).

Theoretisch ist es möglich, dass keine Massnahmen gefunden werden, die ein positives Kosten-Nutzen-Verhältnis aufweisen. Dies kann beispielsweise daran liegen, dass bei der Massnahmenplanung nicht die richtigen Massnahmen angedacht wurden. In diesem Fall sind alternative Massnahmen zur Reduktion der Risiken zu prüfen (gemäss Kapitel 3.4.1). Es kann indessen auch möglich sein, dass es für gewisse Risiken schlicht keine wirksamen und kosteneffizienten Massnahmen gibt. In diesem Fall sind Strategien zum Umgang mit den bestehenden Risiken zu erarbeiten (vgl. nachfolgendes Kapitel).

3.4.3 Beurteilung der verbleibenden Risiken und gesamtheitliche Interessensabwägung

Die nach der gesamtheitlichen Interessensabwägung ermittelte Massnahmenkombination ist anschliessend in Bezug auf das verbleibende Risiko zu beurteilen. Insbesondere ist es wichtig zu prüfen, ob die optimale Massnahmenkombination alle Vorgaben (Gesetze, Richtlinien, Normen, Schutzzielvorgaben usw.) erfüllt. Ist dies nicht der Fall, ist diejenige Massnahmenkombination zu wählen, die der optimalen am nächsten kommt.

Wie aus Abbildung 9 ersichtlich wird, verbleibt bei Erreichen der Grenzkosten nach wie vor ein (beachtliches) Risiko, welchem mit kostenwirksamen Massnahmen nicht entgegengewirkt werden kann. Da sich verbleibende Risiken im Ereignisfall zumindest teilweise als tatsächliche Schäden konkretisieren, ist es wichtig, bereits im Vorfeld eine Strategie im Umgang mit verbleibenden Risiken zu haben. Für betriebliche Risiken bietet sich die Versicherungslösung an, für die gesellschaftlichen und volkswirtschaftlichen Risiken ist insbesondere der Staat gefor-

dert (z. B. im Rahmen der Gefahrenprävention, durch Gewährleistung einer subsidiären Unterstützung im Ereignisfall oder mit der Schaffung eines Solidaritätsfonds usw.). Entsprechende Massnahmen werden u. a. im Rahmen der nationalen SKI-Strategie erarbeitet.

Ein grosses Gewicht ist zudem der Kommunikation der verbleibenden Risiken beizumessen: Ein Risikodialog unter allen Betroffenen erhöht das allgemeine Bewusstsein für Risiken, erweitert die Kenntnisse über diese und sensibilisiert die von den Risiken betroffene Bevölkerung und Wirtschaft. Diese können in vielen Fällen durch selbstvorsorgliche Massnahmen einen wirksamen Beitrag zur Risikoreduktion leisten.

Die Massnahmen müssen nicht nur ökonomisch optimal sein, sondern auch die weiteren Aspekte einer ganzheitlichen Nachhaltigkeit berücksichtigen. Zu diesem Zweck ist zu überprüfen, welche Konsequenzen die vorgeschlagene Massnahmenkombination für die betroffenen Betreiber, die Umwelt, die Wirtschaft und die Gesellschaft nach sich ziehen.

Zudem ist zu klären, wie die Finanzierung der Massnahmen erfolgen soll. Dabei ist insbesondere sicherzustellen, dass keine Wettbewerbsverzerrung respektive Ungleichbehandlung von KI-Betreibern erfolgt (auch in Bezug auf den internationalen Wettbewerb). Da der Fokus beim Schutz kritischer Infrastrukturen auf den Leistungen für die Gemeinschaft liegt, ist auch bei der Finanzierung der Massnahmen darauf zu achten, dass sich die Gemeinschaft an der Risikoreduktion beteiligt (z. B. durch Weiterverrechnung der Kosten an die Kunden oder via öffentliche Hand).

Weiter ist aufzuzeigen, wie die Implementierung der Massnahmen erfolgen soll. Unter Umständen kann es notwendig sein, entsprechende Rechtsgrundlagen zu schaffen respektive zu ergänzen. Es ist abzuklären, welche Rahmenbedingungen diesbezüglich erfüllt sein müssen.

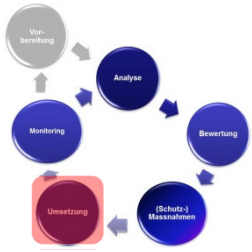
Ergeben sich aus der gesamtheitlichen Interessensabwägung respektive der Beurteilung der verbleibenden Risiken seitens der zuständigen Fachbehörde Vorbehalte gegenüber der vorgeschlagenen Massnahmenkombination, sind die entsprechenden Abklärungen für diejenigen Massnahmenkombinationen vorzunehmen, die der optimalen Massnahmenkombination am nächsten sind. Lassen sich keine Massnahmen bestimmen, die die verschiedenen Ansprüche der gesamtheitlichen Interessenabwägung erfüllen, sind gegebenenfalls die strategische Zielsetzung bzw. die vorgenommenen Bewertungen zu überprüfen (allenfalls vorhandene Schutzziele und Grenzkosten, vgl. Kapitel 3.3).

3.4.4 Verabschiedung der Massnahmen

Die oberste Leitungsorgane (Geschäftsleitung, Verwaltungsrat, Fach-, Aufsichts- und Regulationsbehörden, Kantonsregierung, Bundesrat etc.) haben letztlich zu entscheiden, welche Massnahmen tatsächlich umgesetzt werden sollen. Im Rahmen einer Güterabwägung sind dabei auch noch weitere Interessen zu berücksichtigen (insbesondere die ökologische, wirtschaftliche und gesellschaftliche Nachhaltigkeit, die Verhältnismässigkeit, das Sicherheitsbedürfnis usw.). Deshalb ist es durchaus möglich, dass das tatsächlich realisierte Mass an Sicherheit vom Optimum gemäss Grenzkosten-Ansatz abweicht.

Sind zur Implementierung von Massnahmen Anpassungen von rechtlichen Grundlagen notwendig, erfolgt der abschliessende Entscheid über die zu realisierenden Massnahmen auf politisch-gesellschaftlicher Ebene. Im Rahmen des Rechtsetzungsverfahrens besteht dabei die Möglichkeit, dass interessierte Stellen (insb. Verbände) ihre Anliegen einbringen können (entweder im Vernehmlassungs- oder im Anhörungsverfahren).

3.5 Umsetzung der Massnahmen

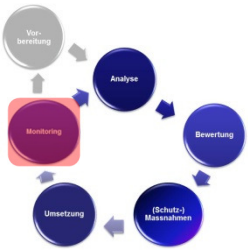


Für die Planung, die Realisierung sowie die Umsetzungskontrolle der Massnahmen ist in der Regel der Betreiber der KI selber verantwortlich.

Wenn das Budget oder die personellen Ressourcen nicht ausreichen, um sämtliche Massnahmen gleichzeitig umsetzen zu können, muss eine Umsetzungsreihenfolge festgelegt werden. Es wird empfohlen, dabei folgende Überlegungen einzubeziehen:

- Enthält ein kritischer Prozess einen *Single-Point-of-Failure*, also eine Stelle, die zu einem Ausfall sämtlicher kritischen Prozesse führen könnte, so ist dieser mit höchster Priorität zu beseitigen bzw. abzusichern.
- Bei einigen Massnahmen ergibt sich durch logische Zusammenhänge eine zwingende zeitliche Reihenfolge bei der Umsetzung.
- Manche Massnahmen sind breitenwirksam, andere wirken eher lokal. Im Rahmen des Schutzes kritischer Infrastrukturen ist es sinnvoll, zuerst auf die Breitenwirkung zu achten.

3.6 Monitoring, Überprüfung und Verbesserung der Massnahmen



Um den integralen Schutz der KI kontinuierlich verbessern zu können, sind nicht nur angemessene Massnahmen umzusetzen und Dokumente fortlaufend zu aktualisieren, sondern auch der integrale Schutz ist regelmässig auf seine Wirksamkeit und Effizienz hin zu überprüfen. Dafür sollte das betriebsintern zuständige leitende Organ periodisch den integralen Schutz kontrollieren und bewerten (Managementbewertung).

Alle Ergebnisse und Beschlüsse sind zudem nachvollziehbar zu dokumentieren. Die Überprüfung und Verbesserung des integralen Schutzes bezieht sich auf alle Phasen; also auf die in der Vorplanung festgelegten Punkte, die Aktualität bestehender Risiken, die Wirksamkeit der umgesetzten Massnahmen sowie die vorbereitenden Massnahmen. Solche Überprüfungen sollten regelmässig erfolgen, z. B. jährlich. Zusätzliche Überprüfungen sind notwendig

- Nach der Umsetzung von Massnahmen,
- nach einem Krisenereignis,
- nach einer Erweiterung/Veränderung in der kritischen Infrastruktur sowie
- bei einer signifikanten Änderung der Gefährdungslage.

3.6.1 Übungen/Tests

Werden Arbeitsabläufe wie etwa die Inbetriebnahme und die Bedienung technischer Einrichtungen nur sporadisch praktiziert, funktionieren sie im Ereignisfall zu langsam und häufig auch fehlerhaft. Die Strukturen und Verfahren der verschiedenen Massnahmen, insbesondere solcher für Ereignisse mit geringer Eintrittswahrscheinlichkeit, aber hohem Schadensausmass, sind daher in regelmässigen Abständen zu testen. Ziele solcher Übungen sind[19]:

- die Überprüfung der Funktionsfähigkeit und Praktikabilität der Massnahmen,
- das Training der Krisenkoordination und -kommunikation,
- der Test der krisenspezifischen Abläufe sowie deren Optimierung anhand praktischer Erfahrungen,
- die Schaffung von Vorgaben zur Entwicklung benötigter Strukturen und Verfahren.

Die Rückkehr vom Notfall- in den Normalbetrieb sollte ebenfalls berücksichtigt werden.

Zur Realisierung von Übungen stehen verschiedene Übungsarten und -methoden zur Verfügung, die sich in Abstraktionsgrad und Übungsaufwand unterscheiden.[20]

3.6.2 Pflege des SKI-Prozesses

Zur Pflege des Prozesses des integralen Schutzes sind für die jeweilige kritische Infrastruktur geeignete Mess- und Bewertungskriterien zu entwickeln. Um die Entwicklung der Werte beobachten zu können, sind regelmässige Messungen notwendig. Bei einer negativen Entwicklung der Werte sind die Ursachen zu ermitteln und Verbesserungsmassnahmen zu definieren, Umsetzungsverantwortliche zu benennen und Anpassungen vorzunehmen.

---

[19] GUSTIN, Joseph F. *Disaster & Recovery Planning: A Guide for Facility Managers,* The Fairmont Press, Lilburn GA, 2004, S. 226.

[20] Anleitungen und Hinweise zu den verschiedenen Übungsarten und -methoden gibt: British Standards Institute – Published Document 25666:2010 – *Business Continuity Management – Guidance on Exercising and Testing for Continuity and Contingency Programmes.*

3.6.3 Überprüfung

Nur durch regelmässige Überprüfungen des integralen Schutzes kann die Fähigkeit der kritischen Infrastruktur, Notfälle und Krisen bewältigen zu können, beurteilt werden. Ziel ist es, die Funktionsfähigkeit, die Effektivität, die Angemessenheit und Effizienz des integralen Schutzes sicherzustellen. Dazu werden Mängel und Verbesserungsmöglichkeiten aufgezeigt sowie Empfehlungen ausgesprochen.

Die Überprüfung des integralen Schutzes sollte auf unterschiedlichen Ebenen erfolgen, z. B. anhand von Selbstbewertungen oder durch interne bzw. externe Revisionen. Die regelmässigen Kontrollen auf den verschiedenen Stufen sind zu planen, durchzuführen und die Ergebnisse zu dokumentieren. Allfällige erkannte Probleme sind zu terminieren und zu beheben.

Abkürzungsverzeichnis

Abkürzung	*Erläuterung*
BBl	Bundesblatt
BCI	*The Business Continuity Institute* → www.thebci.org
BCM	*Business Continuity Management* → Begriffserläuterungen
BIA	Business Impact Analysis → Begriffserläuterungen
BS	British Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik → https://www.bsi.bund.de
IKS	Internes Kontrollsystem → Begriffserläuterungen
ISO	International Organization for Standardization → www.iso.org
KI	Kritische Infrastrukturen → Begriffserläuterungen
SKI	Schutz kritischer Infrastrukturen → Begriffserläuterungen

Abbildungsverzeichnis

Tabellenverzeichnis

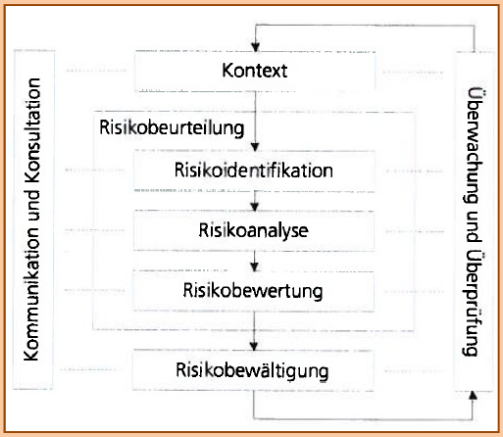
Begriffserläuterungen

Die hier aufgeführten Definitionen geben die Bedeutung der Begriffe wieder, wie sie in diesem Leitfaden verwendet werden. Diese Verwendung kann sich durchaus von jener in anderen Publikationen unterscheiden. Mit einem → wird jeweils auf einen anderen Eintrag in diesen Begriffserläuterungen verwiesen.

Begriff	*Erläuterungen*
Business Impact Analysis (BIA)	Die Business Impact Analysis (dt. Folgeschäden-Abschätzung) ist die Analyse der möglichen Auswirkungen (finanziell/materiell) eines Störfalles auf den ordentlichen Geschäftsbetrieb. Es ist ein Verfahren zur Identifizierung kritischer Ressourcen und Wiederanlaufanforderungen sowie der Auswirkungen von ungeplanten Geschäftsunterbrechungen. *Quelle: Glossar BCMnet.CH, April 2013*
Business Continuity Management (BCM)	Das Business Continuity Management (dt: betriebliches Kontinuitätsmanagement) ist eine ganzheitliche Führungstätigkeit, welche Risiken (und ihre Auswirkungen auf die Geschäftsprozesse) identifiziert, Gegenmassnahmen plant und diese im Störfall einsetzt. Es ist ein Prozess zur Sicherstellung der Fortführung des Geschäftsbetriebs nach Ausfall geschäftskritischer Ressourcen. *Quelle: Glossar BCMnet.CH, April 2013*
Eintrittswahrscheinlichkeit	Als Eintrittswahrscheinlichkeit wird das geschätzte bzw. auf Statistikwerten beruhende Eintreten eines Ereignisses innerhalb einer bestimmten Zeitspanne bezeichnet (z. B. innerhalb von 10 Jahren).
Gefährdung	Als Gefährdung wird eine konkrete Gefahr bezeichnet, die für ein konkretes Schutzgut besteht. Die Gefährdung entspricht daher einem potentiellen Ereignis oder einer potentiellen Entwicklung mit möglichen Auswirkungen für ein Schutzgut. *Quelle: Glossar der Risikobegriffe, Bundesamt für Bevölkerungsschutz BABS, 29.4.2013*
Grenzkosten	Die Grenzkosten sind ein Mass für die Zahlungsbereitschaft, um risikoreduzierende Massnahmen zu ergreifen. Konkret bezeichnen sie die Kosten pro verhinderte Schadenseinheit, welche die Gesellschaft höchstens aufzuwenden bereit ist, um Massnahmen zur Reduktion von Risiken (→ Risiko) zu ergreifen. *Quelle: Glossar der Risikobegriffe, Bundesamt für Bevölkerungsschutz BABS, 29.4.2013*
Internes Kontrollsystem (IKS)	Beim internen Kontrollsystem handelt es sich um die Gesamtheit aller Prozesse, Methoden und Kontrollmassnahmen, die dazu dienen, einen ordnungsgemässen Ablauf des betrieblichen Geschehens sicherzustellen. Für privatrechtliche Unternehmen begründet sich das interne Kontrollsystem im Obligationenrecht, Art. 716a. Für die Bundesverwaltung ist das interne Kontrollsystem im Finanzhaushaltgesetz (FHG Art. 39) sowie in der Finanzverordnung (FHV, Art. 36) beschrieben. Das IKS behandelt operative Risiken (→ Risiko) im Bereich der finanziellen und wirtschaftlichen Risiken sowie rechtliche Risiken (Konformität mit anzuwendenden Regeln (Compliance)). *Quelle: Glossar der Risikobegriffe, Bundesamt für Bevölkerungsschutz BABS, 29.4.2013*
Kernprozess	Kernprozesse sind Prozesse (→ Prozess), die direkt einen Beitrag zum Erfüllen der Aufgabe der kritischen Infrastruktur liefern. Diese Prozesse können beispielsweise die Erfüllung der übertragenen staatlichen Aufgaben bei Behörden sein, die Erbringung von Dienstleistungen oder auch die Herstellung eines Produkts.
Kontinuitätsmanagement	Siehe: Business Continuity Management
Kosten-Wirksamkeit	Die Kosten-Wirksamkeit ist ein Mass für die Verhältnismässigkeit von Massnahmen. Sie ist damit ein Merkmal von Massnahmen und setzt die

	→ Wirksamkeit der Massnahmen (→ Risikominderung) den entstehenden Kosten gegenüber. *Quelle: Glossar der Risikobegriffe, Bundesamt für Bevölkerungsschutz BABS, 29.4.2013*
Krisenmanagement	Systematische Vorsorge für Krisen sowie deren Bewältigung. Krisenmanagement beinhaltet die Krisenorganisation, die Identifikation und Analyse von Krisensituationen, die Entwicklung von Strategien zur Bewältigung der Krisen sowie die Einleitung und Verfolgung von Gegenmassnahmen. Das Krisenmanagement umfasst sowohl die Vorbereitung auf die Krisensituation als auch die Steuerung in der Situation selbst. *Quelle: Glossar der Risikobegriffe, Bundesamt für Bevölkerungsschutz BABS, 29.4.2013*
Kritische Infrastrukturen (KI)	Als kritische Infrastrukturen werden Prozesse, Systeme und Einrichtungen bezeichnet, die essenziell für das Funktionieren der Wirtschaft bzw. das Wohlergehen der Bevölkerung sind.
Kritischer Prozess	Im Rahmen des Schutzes kritischer Infrastrukturen wird unter kritischem Prozess ein Prozess verstanden, welcher für die Funktionsfähigkeit der kritischen Infrastruktur existenziell wichtig ist und bei dessen Ausfall die Bevölkerung und deren Lebensgrundlagen in einem schweren Masse betroffen wären.
Lebensgrundlage	Die Lebensgrundlage ist die Gesamtheit der Elemente, die für das Leben der Bevölkerung notwendig sind. Die Lebensgrundlagen ermöglichen das kollektive und individuelle Zusammenleben. Sie lassen sich in natürliche, wirtschaftliche und gesellschaftliche Lebensgrundlagen unterteilen: - Natürliche Lebensgrundlagen: intakte Umwelt (Boden, Wasser, Luft, Biodiversität) - Wirtschaftliche Lebensgrundlagen: prosperierende Wirtschaft und funktionierende Infrastrukturen - Gesellschaftliche Lebengrundlagen: funktionierendes Rechtssystem und verfassungsmässige Ordnung, gegenseitiges Vertrauen, territoriale Integrität und kulturelle Vielfalt. *Quelle: Glossar der Risikobegriffe, Bundesamt für Bevölkerungsschutz BABS, 29.4.2013*
Notfallmanagement	Mit einem Notfallmanagement (auch Notfallvorsorge genannt) wird eine Organisation darauf vorbereitet, auf eine Notsituation rasch zu reagieren und diese zu bewältigen. Im Notfallmanagement werden z. B. die Notfallorganisation, die Alarmierungsabläufe, die schematische Reaktion (Sofortmassnahmen) auf bestimmte Notsituationen und Verhaltensanweisungen festgelegt und geschult sowie die Zusammenarbeit mit den Blaulichtorganisationen dokumentiert. Ziel ist es, im Notfall keine Zeit für unnötige Entscheidungen, Anweisungen und die Zuweisung von Kompetenzen zu verlieren. Im Notfallmanagement steht der Schutz von Leib und Leben im Vordergrund. Da es der Bewältigung von Ereignissen dient, kann es aber auch als Teil des → Business Continuity Management (BCM) aufgefasst werden oder als Teil des → Krisenmanagements, weil Notsituationen als Ausgangspunkt von Krisen aufgefasst werden können.
Prozess	Ein Prozess kann als Abfolge von (Teil-)Prozessen gesehen werden, in denen Aktionen ausgeführt und Entscheidungen getroffen werden. Ein Prozess benötigt in der Regel Eingaben (Input), die von anderen Geschäftsprozessen geliefert werden. Ein Prozess liefert Ergebnisse (Output) beispielsweise in Form von Produkten, Informationen oder Dienstleistungen. In- und Output stellen die Verbindungen zwischen den Prozessen dar. Geschäftsprozesse werden ihrer Art gemäss in → Kernprozesse und → Supportprozesse unterteilt.
Resilienz	Die Resilienz beschreibt die Fähigkeit eines Systems, einer Organisation oder einer Gesellschaft, intern oder extern verursachten Störungen zu widerstehen und die Funktionsfähigkeit möglichst zu erhalten respektive

	wieder zu erlangen. Die Resilienz setzt sich aus vier Bestandteilen zusammen: 1) die Robustheit der Systeme (z. B. → kritische Infrastrukturen, Staat, Wirtschaft und Gesellschaft) an sich; 2) die Verfügbarkeit von Redundanzen; 3) die Fähigkeit, wirksame Hilfsmassnahmen zu mobilisieren; 4) die Schnelligkeit und Effizienz der Hilfsmassnahmen. *Quelle: Glossar der Risikobegriffe, Bundesamt für Bevölkerungsschutz BABS, 29.4.2013*
Risiko	Das Risiko ist ein Mass für die Grösse einer → Gefährdung und beinhaltet die → Eintrittswahrscheinlichkeit und das → Schadensausmass eines unerwünschten Ereignisses. *Quelle: Glossar der Risikobegriffe, Bundesamt für Bevölkerungsschutz BABS, 29.4.2013* Der Begriff Risiko dient beim → Schutz kritischer Infrastrukturen als Modell sowohl zur Beurteilung von Sicherheitsfragen als auch zum Vergleich verschiedener → Gefährdungen anhand gleicher Kriterien. Das Risikomodell beruht grundsätzlich auf zwei Faktoren: → Eintrittswahrscheinlichkeit eines Ereignisses; → Schadensausmass an Bevölkerung und deren → Lebensgrundlagen. Risiken lassen sich demzufolge als Produkt darstellen, das durch die Eintrittswahrscheinlichkeit eines Ereignisses und dessen Schadensausmasses bestimmt ist.
Risikoanalyse	Die Risikoanalyse erfasst und beschreibt systematisch die Risiken (→ Risiko) in einem betrachteten System. Dazu gehört die Einschätzung der Höhe der Risiken, oft in Form einer Einstufung der betrachteten Szenarien bzgl. ihrer → Eintrittswahrscheinlichkeit und ihres → Schadensausmasses. Die Risikoanalyse befasst sich mit der Frage «was kann passieren?». *Quelle: Glossar der Risikobegriffe, Bundesamt für Bevölkerungsschutz BABS, 29.4.2013* Die Risikoanalyse ist die Grundlage zum → Risikomanagement. Sie dient der Beschreibung des Wesens des → Risikos und der Bestimmung der Risikohöhe (ÖNORM ISO:3100). Mit der Risikoanalyse wird eine möglichst konkrete und transparente Ausgangslage für das Planen von Schutzmassnahmen geschaffen. Dafür werden in einem ersten Schritt alle potenziellen Risiken, die der Organisation schaden können, identifiziert und aufgelistet. Für die ausgewählten Risiken werden die Auswirkungen (in der Regel finanzieller Art) für die jeweilige Betrachtungsebene (z.B. Unternehmen oder Gemeinschaft) und die Eintrittswahrscheinlichkeit geschätzt. Die Auswirkungen und die Eintrittswahrscheinlichkeit von Risiken hängen von den Annahmen über deren Intensität ab, die der Schätzung zugrunde liegen. Daher ist es für die Schätzung notwendig, ein Szenario für die einzelnen Risiken zu definieren. Der Einfachheit halber wird in der Regel vom schlimmsten möglichen Fall ausgegangen, der aber noch denkbar ist (*worst credible case*). Die Risikohöhe wird durch das Produkt von Schadensausmass und Eintrittswahrscheinlichkeit bestimmt. Diese Resultate lassen sich in einer Risikomatrix darstellen, die dem Risikomanagement als Planungsgrundlage dient.
Risikomanagement	Unter Risikomanagement werden die koordinierten Aktivitäten zur Steuerung und Lenkung einer Organisation in Bezug auf Risiken, d. h. auf Auswirkungen von Unsicherheiten auf die Ziele der Organisation verstanden. *Quelle: ÖNORM ISO 31000:2010* Das Risikomanagement ist ein systematischer Prozess für eine umfassende Behandlung von Risiken. Das Risikomanagement ist ein etablierter Prozess in Gesellschaft und Wirtschaft im Umgang mit Risiken. Je nach

	Kontext wird das Risikomanagement unterschiedlich aufgebaut und betrieben (Elemente und Gewichtungen). Als allgemeingültiger Vertreter ist nachfolgend der Prozess gemäss ISO 3100 dargestellt.  *Quelle: Glossar der Risikobegriffe, Bundesamt für Bevölkerungsschutz BABS, 29.4.2013*
Risikominderung	Massnahmen zur Risikominderung reduzieren entweder die Verwundbarkeit der Risikoelemente gegenüber der Einwirkung von Gefahren oder richten sich unmittelbar an die betriebliche Kontinuität der kritischen Prozesse durch die Schaffung von Redundanz beziehungsweise Ersatz. Redundante Systeme oder Ersatzsysteme ermöglichen die betriebliche Kontinuität kritischer Prozesse im Rahmen des Wiederanlaufmanagements, auch wenn es zur Beeinträchtigung von Risikoelementen kommt. *Quelle: Bundesministerium des Inneren, Schutz kritischer Infrastrukturen – Risiko-und Krisenmanagement – Leitfaden für Unternehmen und Behörden, Berlin, Januar 2008, S. 21-22.*
Risikovermeidung	Risiken können vermieden werden, indem man entweder gefährdete Regionen meidet oder Massnahmen umsetzt, die dazu führen, dass Gefährdungen nicht entstehen können. Exponierte, also gefährdete Bereiche können im Hinblick auf Naturgefahren oder im Umfeld risikobehafteter Anlagen häufig benannt werden. Es besteht die Möglichkeit, bei einer Neuplanung von Standorten oder Einzelgebäuden und Anlagen solche Bereiche zu meiden. Eine vollständige Vermeidung von Risiken ist jedoch nicht möglich, da kein Standort risikofrei ist. *Quelle: Bundesministerium des Inneren, Schutz kritischer Infrastrukturen – Risiko-und Krisenmanagement – Leitfaden für Unternehmen und Behörden, Berlin, Januar 2008, S. 21-22.*
Schadensausmass	Als Schadensausmass werden die geschätzten Auswirkungen auf die Bevölkerung und deren → Lebensgrundlagen bezeichnet, die durch den Ausfall eines oder mehrerer → kritischer Prozesse bei Eintritt der → Gefährdung entstehen. Es besteht aus der Summe des Schadens zum Zeitpunkt des Eintritts eines Ereignisses und des Schadens, der während der ganzen Wiederherstellungszeit entstehen kann.
Schutz kritischer Infrastrukturen (SKI)	Der Schutz kritischer Infrastrukturen umfasst Massnahmen, die die → Eintrittswahrscheinlichkeit und/oder das → Schadensausmass einer Störung, eines Ausfalls oder einer Zerstörung von → kritischen Infrastrukturen reduzieren beziehungsweise die Ausfallzeit minimieren. *Quelle: Glossar der Risikobegriffe, Bundesamt für Bevölkerungsschutz BABS, 29.4.2013*
Schutzziel	Ein Schutzziel bezeichnet das Niveau an Sicherheit, das bestimmte Verantwortungsträger in ihrem Verantwortungsbereich grundsätzlich anstreben. *Quelle: Sicherheitsniveau für Naturgefahren, PLANAT 2013*
Schwerwiegende Ausfälle	Ein Ausfall ist schwerwiegend, wenn wichtige Güter und Dienstleistungen während längerer Zeit im Gebiet, in dem die KI jeweils relevant ist (Gemeinde, Kanton, Region, Land usw.) nicht verfügbar sind.

Sicherheitsmanagement	Das Sicherheitsmanagement bezeichnet die Planung, die Steuerung und die Kontrolle der Sicherheit in einer Organisation. Es umfasst Aspekte der Sicherheit von technischen Systemen, nicht-technische Aspekte, z. B. der Arbeitssicherheit oder Betriebssicherheit, sowie die Sicherheit von Räumen und Gebäuden. Das Sicherheitsmanagement wird z. T. als übergeordneter Prozess verstanden, in dem Komponenten wie → Risikomanagement, → Business Continuity Management (BCM) usw. integriert sind. Es existieren aber auch Organisationsformen, in denen das Sicherheitsmanagement als eine Massnahme im Bereich des → Risikomanagements integriert wird.
Sicherheitsniveau	Der von allen Verantwortungsträgern gemeinsam erstrebte Sicherheitszustand. *Quelle: Sicherheitsniveau für Naturgefahren, PLANAT 2013*
Single Point of Failure	Gravierende Fehlerquelle, die zu einem Komplettausfall der kritischen Infrastruktur bzw. deren kritischer Prozesse führt. Solche Fehlerquellen sind mit höchster Priorität zu beseitigen bzw. abzusichern.
SKI-Inventar	Das SKI-Inventar ist ein Verzeichnis derjenigen KI-Objekte, deren Ausfall, Störung oder Zerstörung die Bevölkerung und ihre Lebensgrundlagen in schwerwiegendem Masse beeinträchtigen könnte. Zum einen handelt es sich dabei um Objekte mit grosser Bedeutung bei der Versorgung mit wichtigen Gütern und Dienstleistungen, zum andern um Objekte, die ein grosses Gefahrenpotenzial darstellen. Unter anderem sind im Inventar KI-Objekte erfasst, die auf nationaler Ebene von Bedeutung sind. Das SKI-Inventar ersetzt den Objektkatalog SEB (Sicherstellung Existenzieller Bedürfnisse), der im Rahmen der früheren Gesamtverteidigung erhoben und aktualisiert wurde. Das SKI-Inventar wurde unter der Leitung des Bundesamtes für Bevölkerungsschutz BABS in enger Zusammenarbeit mit den zuständigen Stellen des Bundes, den Kantonen und den KI-Betreibern erstellt und wird regelmässig aktualisiert. Das Inventar soll vor allem als Grundlage für Planungs- und Entscheidungsprozesse auf den verschiedenen Stufen (Bund, Kantone und KI-Betreiber) dienen.
Supportprozess	Supportprozesse tragen nicht direkt zur Erfüllung der Aufgaben einer kritischen Infrastruktur bei, können jedoch indirekt eine sehr wichtige und damit eine kritische Rolle spielen, da sie der Aufrechterhaltung von → Kernprozessen dienen. Zu den Supportprozessen eines KI-Objekts zählen z. B. die Stromversorgung und die Telekommunikation.
Teilsektor	Die → kritischen Infrastrukturen in der Schweiz wurden in 28 Teilsektoren unterteilt. Diese Teilsektoren umfassen die verschiedenen Branchen, Industrien, Wirtschaftssektoren und sonstige wirtschaftliche Unterteilungen. Folgende Teilsektoren existieren im Bereich der kritischen Infrastrukturen in der Schweiz: Abfälle, Abwasser, Armee, Ärztliche Betreuung und Spitäler, Diplomatische Vertretungen und Sitze internationaler Organisationen, Banken, Blaulichtorganisationen, Chemie- und Heilmittelindustrie, Erdgasversorgung, Erdölversorgung, Forschung und Lehre, Informationstechnologien, Kulturgüter, Labors, Lebensmittelversorgung, Luftverkehr, Maschinen-, Elektro- und Metallindustrie, Medien, Parlament – Regierung – Justiz – Verwaltung, Postverkehr, Schienenverkehr, Schiffsverkehr, Strassenverkehr, Stromversorgung, Telekommunikation, Versicherungen, Wasserversorgung und Zivilschutz.
Unternehmensweite Sicherheitspolitik	Ein zentrales und tragendes Element bei der Etablierung einer ganzheitlichen Unternehmenssicherheit ist die Formulierung einer unternehmensweiten Sicherheitspolitik (engl. *Corporate Security Policy*). Der Begriff Sicherheitspolitik wird in den verschiedenen Normen, Standards und in der Literatur unterschiedlich definiert. Grundsätzlich legt sie die Sicherheitsausrichtung und -kultur sowie die Sicherheitsstandards und -regelungen innerhalb einer Organisation fest.

	Aus ihr lassen sich Schutzziele herleiten, indem sie das angestrebte Sicherheitsniveau beschreibt (ISO/IEC TR 13335-1). Die unternehmensweite Sicherheitspolitik widerspiegelt die Unternehmenspolitik und sollte von der Leitungsebene herausgegeben und unterzeichnet sein. In der Sicherheitspolitik übernimmt die Leitungsebene die Verantwortung für die Unternehmenssicherheit (Müller, 2005). Die unternehmensweite Sicherheitspolitik muss innerhalb des Unternehmens publiziert werden und sie muss jedem bekannt sein. Sie ist kurz gefasst, klar und verständlich formuliert und auf wenige Seiten beschränkt. Eine unternehmensweite Sicherheitspolitik enthält u. a. folgende Aspekte: - Stellenwert der Sicherheit im Unternehmen - Referenzierung auf übergeordnete Anforderungen und geltende Gesetze - Sicherheitsziele und die dafür benötigten Strategieelemente sowie anzuwendende Methoden / Standards - Elemente der Sicherheitsorganisation - Aussagen zur Überprüfung der Umsetzung der unternehmensweiten Sicherheitspolitik - Aussagen zur Konsequenz bei Nichteinhaltung der unternehmensweiten Sicherheitspolitik
Verbleibendes Risiko	Das verbleibende Risiko (auch Restrisiko) bezeichnet das → Risiko, das nach Realisierung aller vorgesehenen Sicherheitsmassnahmen weiterhin verbleibt. *Quelle: Glossar der Risikobegriffe, Bundesamt für Bevölkerungsschutz BABS, 29.4.2013*
Wirksamkeit	Die Wirksamkeit bezieht sich auf Massnahmen und gibt an, um wie viel das → Risiko durch die Massnahmen reduziert wird. *Quelle: Glossar der Risikobegriffe, Bundesamt für Bevölkerungsschutz BABS, 29.4.2013*

Anhang 1 – Methodische Grundlagen

Australien/Neuseeland:

- AS/NZS 4360:2004 *Risk management* (replaced by AS/NZS ISO 31000:2009).
- HB 436:2004 *Risk Management Guidelines Companion to AS/NZS 4360:2004.*
- AS/NZS 5050:2010 *Business Continuity – Managing Disruption Related Risks.*
- HB 221:2004 *Business Continuity Management*.

Deutschland:

- BBK: *Schutz kritischer Infrastruktur – Risikomanagement im Krankenhaus*, 2008. http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Praxis_Bevoelkerungsschutz/Band_2_Praxis_BS_Risikomanagm_Krankenh_Kritis.pdf?__blob=publicationFile
- BBK: *Methode für eine Risikoanalyse im Bevölkerungsschutz*, 2010. http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Wissenschaftsforum/Bd8_Methode-Risikoanalyse-BS.pdf;jsessionid =4914E21B99FB591B6EC2A0CCDBB766CD.1_cid345?__blob=publicationFile
- BMI: *Schutz kritischer Infrastrukturen – Risiko- und Krisenmanagement – Leitfaden für Unternehmen und Behörden*, 2. Auflage, 2011. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2008/Leitfaden_Schutz_kritischer_Infrastrukturen.html?nn=3314962
- BSI-Standard 100-4: *Notfallmanagement, Version 1.0, 2008 (Fokus auf IT-Service Continuity Management).* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1004_pdf.pdf?__blob=publicationFile
- *Umsetzungsrahmenwerk zum Notfallmanagement nach BSI-Standard 100-4*, 2013 (Fokus auf IT-Service Continuity Management). https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Umsetzungsrahmenwerk/umra.html

Europäische Union:

- Commission Staff Working Paper SEC (2010) 1626 final: *Risk Assessment and Mapping Guidelines for Disaster Management*, 2010. http://ec.europa.eu/echo/files/about/COMM_PDF_SEC_2010_1626_F_staff_working_document_en.pdf
- European Network and Information Security Agency (ENISA): *Good Practice Guide for Incident Management*, 2010. http://www.enisa.europa.eu/act/cert/support/incident-management/files/good-practice-guide-for-incident-management/at_download/fullReport

International Organization for Standardization (ISO):

- ISO/IEC 13335-1:2004: *Information Technology – Security Techniques – Management of Information and Communications Technology Security – Part 1: Concepts and Models for Information and Communications Technology Security Management.*
- ISO 22301:2012 – *Societal Security – Business Continuity Management Systems – Requirements.*
- ISO 22313:2012 – *Societal Security – Business Continuity Management Systems – Guidance. First edition, 15. December 2012.*
- ISO 22320:2011 – *Sicherheit und Schutz des Gemeinwesens – Management der Gefahrenabwehr – Anforderungen an die Führungsstrukturen*, 2011.
- ISO 22399:2007 – *Societal Security – Guideline for incident preparedness and operational continuity management.*
- ISO/IEC 27001:2005 – *Information technology – Security Techniques – Information Security Management Systems – Requirements.*
- ISO/IEC 27002:2005 – *Information Technology – Security Techniques – Code of Practice for Information Security Management.*
- ISO 31000: 2009 – *Risk Management: Principles and Guidelines.*

Österreich:

- Austrian Standards Institute: *ONR 49000:2010 ff Risikomanagement für Organisationen und Systeme.* (Familie bestehend aus: ONR 49000, 49001, 49002-1, ONR 49002-2, 49002-3, 49003).

Schweiz:

- BABS: *Kantonale Gefährdungsanalyse und Vorsorge. Leitfaden KATAPLAN. Januar 2013.*
  http://www.kataplan.ch
- BABS: *Nationale Gefährdungsanalyse «Katastrophen und Notlagen Schweiz» – Risikobericht 2012.*
  http://www.risk-ch.ch → Downloads
- BABS: *Methode zur Risikoanalyse von Katastrophen und Notlagen für die Schweiz,* Version 1.03, Stand: 17. April 2013.
  http://www.risk-ch.ch → Downloads
- BABS: Integrales Risikomanagement. Bedeutung für den Schutz der Bevölkerung und ihrer Lebensgrundlagen, 2014.
- BABS: *Führungsbehelf für Angehörige von zivilen Führungsorganen*, Dok 1300-00-5-d, 2010.
  http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/dokumente/aubildungsunterlagen/fuehrungsbehelf_fuer.html
- BABS / PLANAT: *Risikoaversion: Entwicklung systematischer Instrumente zur Risiko- bzw. Sicherheitsbeurteilung – Zusammenfassender Bericht*, 2008.
- http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/gefaehrdungen-risiken/studien/risiko-aversion.htmlBABS: *Glossar der Risikobegriffe,* Stand: 29. April 2013
- BCMnet.CH (Business Continuity Management Network Switzerland): *Glossar, Version 1.1*, April 2013.
  http://www.bcmnet.ch/downloads/Publikationen/BCMnet-Glossar-V1.1-1.4.14.pdf
- BWL: *BCM-Ratgeber*: *Unternehmenserfolg nachhaltig sichern – auch im Krisenfall*, Bestell-Nr. 750.142.d, November 2011.
  http://www.bwl.admin.ch/dienstleistungen/01197/index.html?lang=de&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDdXt9fGym162epYbg2c_JjKbNoKSn6A--
- EFV: *Handbuch zum Risikomanagement Bund,* Version vom 29. April 2013.
  http://www.efv.admin.ch/d/downloads/finanzpolitik_grundlagen/risiko_versicherungspolitik/Handbuch_Risikomanagement_Bund.pdf
- GRF Davos: Schutzziele für kritische Infrastrukturen – Grundlagenbericht. Forschungsauftrag Nr. 353003897-SFA des Bundesamtes für Bevölkerungsschutz BABS, Bern. September 2013.
- *Nationale Strategie zum Schutz kritischer Infrastrukturen 2018 – 2022 (BBl 2018 503-540).*
  http://www.infraprotection.ch → Publikationen
- *Nationale Strategie zum Schutz kritischer Infrastrukturen vom 27. Juni 2012 (BBl 2012 7715-7739).*
  http://www.infraprotection.ch → Publikationen
- PLANAT: *Synthesebericht «Strategie Naturgefahren Schweiz»,* 2004.
- PLANAT: *Risikokonzept Naturgefahren – Leitfaden,* 2009.
- PLANAT: *Sicherheitsniveau für Naturgefahren,* August 2013
- Schweizerische Bankiervereinigung: *Empfehlungen für das Business Continuity Management, 2007.*
  http://www.swissbanking.org/11107_d.pdf
- VBS: *Weisungen über die Massnahmen zur Aufrechterhaltung der Führungsfähigkeit des VBS (WBCM) vom 3. November 2011.*
- VBS/IOS: *Weisungen über das Integrale Schutzkonzept VBS (WISK, 94.102) vom 12. November 2012.*

- *Weisungen über die Risikopolitik des Bundes vom 24. September 2010 (BBl 2010 6549).*
  http://www.admin.ch/opc/de/federal-gazette/2010/6549.pdff

UK:

- Business Continuity Institute: *Good Practice Guidelines* – 2010.
- British Standards Institute: BS 25999-1:2006 – *Business Continuity Management – Code of Practice.*
- British Standards Institute: BS 25999-2:2007 – *Specification for Business Continuity Management.*
- British Standards Institute: PAS 200:2011 – *Crisis Management. Guidance and Good Practice.*
- British Standards Institute: BS 31100:2011 – *Risk Management – Code of Practice and Guidance for the Implementation of BS ISO 31000.*
- British Standards Institute: Published Document 25666:2010 – *Business Continuity Management – Guidance on Exercising and Testing for Continuity and Contingency Programmes*, 2010.
- Center for the Protection of National Infrastructure: *Personnel Security Risk Assessment – A Guide,* 4th edition, 2013.
  http://www.cpni.gov.uk/documents/publications/2010/2010037-risk_assment_ed3.pdf?epslanguage=en-gb
- Center for the Protection of National Infrastructure: *Guide to Producing Operational Requirements for Security Measures*, 2013.
  http://www.cpni.gov.uk/documents/publications/2010/2010001-op_reqs.pdf?epslanguage=en-gb
- Financial Services Authority (FSA): *Business Continuity Management Practice Guide,* 2006.
  http://www.fsa.gov.uk/pubs/other/bcm_guide.pdf
- The Institute of Risk Management: *A Risk Management Standard*, 2002.

USA:

- American National Standard: ASIS SPC.1-2009 – *Organizational Resilience: Security Preparedness, and Continuity Management Systems-Requirement with Guidance for Use*, 2009.
- National Fire Protection Association: NFPA 1600: *Standard on Disaster / Emergency Management and Business Continuity Programs*, 2010.
- Department of Homeland Security: *National Infrastructure Protection Plan*, 2013.
  https://www.dhs.gov/national-infrastructure-protection-plan

Weitere Autoren und Herausgeber:

- GUSTIN, Joseph F.: *Disaster & Recovery Planning: A Guide for Facility Managers*, The Fairmont Press, Lilburn GA, 2004.
- PricewaterhouseCoopers AG: *Internes Kontrollsystem – Führungssystem im Wandel*, 2007.
- Schweizerische Rückversicherungsgesellschaft Swiss Re: *«Präventive Schadenbewältigung: Mehr gewinnen als verlieren»*, 2001.

Anhang 2 – Schadensindikatoren

Die nachstehenden 12 Schadensindikatoren sind der *Methode zur Risikoanalyse von Katastrophen und Notlagen für die Schweiz, Version 1.03* entnommen.

Anh 2.1 – Todesopfer

Beschreibung

Personen, deren Tod sich auf das Ereignis oder dessen Entwicklung zurückführen lässt.

A1	A2	A3	A4	A5	A6	A7	A8
0 – 1	2 – 3	4 – 10	11 – 30	31 – 1'00	101 – 3'00	301 – 1'000	> 1'000

Anh 2.2 – Verletzte/Kranke

Beschreibung

Personen, deren Verletzung oder Krankheit sich auf das Ereignis oder dessen Entwicklung zurückführen lässt. Der Indikator umfasst alle Formen von physischen und psychischen Krankheiten oder Verletzungen, die mit der Gefährdung in Verbindung stehen. Es werden folgende Stufen unterschieden:

	Verletzung	Erkrankung	Faktor
schwer	Spitalaufenthalt von mindestens 7 Tagen. Keine bleibenden körperlichen Schäden.	Chronische Erkrankung, medizinische Behandlung erforderlich.	1
mittel-schwer	Spitalaufenthalt von 1 bis 6 Tagen. Keine bleibenden körperlichen Schäden.	Schwere, lang anhaltende Erkrankung mit vollständiger Genesung, medizinische Behandlung erforderlich.	0.1
leicht	Keine bleibenden körperlichen Schäden, medizinische Behandlung, aber kein Spitalaufenthalt.	Leichte Erkrankung mit vollständiger Genesung, medizinische Behandlung erforderlich.	0.003

Die unterschiedlichen Schweregrade von Verletzungen werden durch die angegebenen Umrechnungsfaktoren berücksichtigt.

A1	A2	A3	A4	A5	A6	A7	A8
≤ 10	101–30	31–100	101–300	301–1000	1001–3000	3001–10000	> 10'000

Personen, die ihren Verletzungen oder ihrer Krankheit erliegen, erfasst nicht dieser Indikator, sondern der Indikator «Todesopfer».

Anh 2.3 – Unterstützungsbedürftige

Beschreibung

Der Indikator erfasst Personen, die vor, während und/oder nach einem Ereignis zu evakuieren, temporär unterzubringen und/oder anderweitig zu betreuen sind. Es handelt sich dabei beispielsweise um das Unterbringen in Notunterkünften, das Versorgen von Personen in von der Aussenwelt abgeschnittenen Ortschaften mit Lebensmitteln oder die kurzfristige psychologische Betreuung (psychologische Nothilfe) von Personen, die jedoch keine eigentliche physische Krankheit erleiden. Erfasst wird die Dauer der Unterstützungsbedürftigkeit der direkt betroffenen Personen. Auswirkungen wie Versorgungsengpässe und -unterbrüche für grössere Bevölkerungsteile werden mit dem Indikator «Versorgungsunterbrüche und -engpässe» erfasst.

Die Unterstützungsbedürftigkeit wird in der Einheit Personentage angegeben. Darunter wird das Produkt aus der Anzahl unterstützungsbedürftiger Personen und der Dauer der Beeinträchtigung in Tagen verstanden. Es wird die effektive Dauer der Unterstützungsbedürftigkeit über die betroffenen Personen zusammengezählt. Pro Person ist die Mindestdauer ein Tag. Erfasst wird die Dauer, über die eine Unterstützungsbedürftigkeit besteht, nicht jedoch die Dauer, über welche die Unterstützungsleistungen bereitgestellt werden. So wird z. B. gezählt, über wie viele Tage die betroffene Anzahl traumatisierter Personen nach einem Ereignis psychologische Nothilfe benötigen, und nicht die Dauer, in welcher die Mitglieder der Betreuung leistenden Organisationen im Einsatz sind. Die Kosten für die Erbringung der Unterstützungsleistung berücksichtigt der Indikator «Vermögensschäden und Bewältigungskosten».

A1	A2	A3	A4	A5	A6	A7	A8
≤ 20'000	20'001–60'000	60'001–200'000	200'001–600'000.	600'001–2 Mio.	> 2–6 Mio.	> 6–20 Mio.	> 20 Mio.

Anh 2.4 – Geschädigte Ökosysteme

Beschreibung

Der Indikator gibt an, wie gross die Land- und/oder Wasserfläche ist, die von einer schädlichen Einwirkung betroffen ist, z. B. durch Freisetzung schädlicher Stoffe.

Als geschädigt gilt ein Ökosystem, in dem

a) das natürliche Gleichgewicht massiv gestört wird und sich die Systeme regenerieren müssen:

und/oder

b) wichtige Ökosystemleistungen deutlich eingeschränkt sind. (z. B. wenn sich Oberflächengewässer nicht mehr zur Trinkwasserversorgung eignen).

Auswirkungen können beispielsweise durch chemische oder radiologische Belastungen, Kontaminationen mit invasiven Neobiota oder physischen Beeinträchtigungen, z. B. durch Erosion, hervorgerufen werden.

Beeinträchtigungen werden in der Einheit *Flächenjahr (km^2 x Jahr)* angegeben. Darunter wird das Produkt der betroffenen Fläche mit der Anzahl Jahre der Beeinträchtigung verstanden. Ist eine Fläche von mehreren Auswirkungen betroffen, wird diese nur einmal erfasst.

Folgen der Schädigung der Ökosysteme werden hier nicht berücksichtigt (z. B. Einschränkungen der Versorgung mit lebensnotwendigen Gütern und Dienstleistungen, wie z. B. ein Versorgungsengpass mit Trinkwasser, bis entsprechende Logistik bereitsteht). Dies wird durch andere Indikatoren (z.B. Beeinträchtigung Lebensqualität) erfasst.

A1	A2	A3	A4	A5	A6	A7	A8
≤ 15	16–45	> 45–150	> 150–450	> 450–1500	> 1500–4500	> 4500–15'000	> 15'000

Anh 2.5 – Vermögensschäden und Bewältigungskosten

Beschreibung

Der Schadensindikator misst die Schäden an bestehenden Vermögenswerten sowie die Kosten der Bewältigung.

Das Vermögen besteht zum einen aus Anlagegütern und zum anderen aus finanziellem Vermögen. Der Indikator erfasst alle Schäden am Vermögen, auch wenn beispielsweise Versicherungsunternehmen oder der Staat die Kosten ausgleichen.

Zu den Kosten der Bewältigung sind z. B. die Kosten für Einsatzkräfte, für Notunterkünfte und die Versorgung der Unterstützungsbedürftigen zu zählen.

Beispiel Hochwasser: Ein Hochwasser verursacht Schäden an mehreren Gebäuden und einem Produktionsbetrieb. Es entstehen Kosten durch das Auspumpen von Kellern und die Beseitigung von Geschiebe und Schwemmholz (Bewältigungskosten). Der Sachschaden ist ein Vermögensschaden, da die Gebäude und Anlagen nun weniger wert sind.

Je nach den Auswirkungen der Gefährdungen kann zur Abschätzung der Vermögensschäden ein unterschiedlicher Blickwinkel gewählt werden:

• Gesamtwirtschaftlich: Schweizweite Bewältigungskosten und Schäden am Volksvermögen.

• Individuell oder kleinräumlich: Bewältigungskosten und Vermögensschäden für Individuen oder in einer räumlich begrenzten Einheit.

A1	A2	A3	A4	A5	A6	A7	A8
≤ 5 Mio.	6–15 Mio.	> 15–50 Mio.	> 50 Mio.–150 Mio.	> 150 Mio. – 500 Mio.	> 500 Mio. – 1,5 Mrd.	> 1,5–5 Mrd.	> 5 Mrd.

Anh 2.6 – Reduktion der wirtschaftlichen Leistungsfähigkeit

Beschreibung

Der Schadensindikator umfasst indirekte wirtschaftliche Auswirkungen, welche die Wertschöpfung in der Schweiz reduzieren.

Während der Indikator «Vermögensschäden und Bewältigungskosten» (vgl. Anh 2.5) also die Kosten der Bewältigung und die Schäden am bestehenden Vermögen erfasst, berücksichtigt dieser Indikator die Folgen für die künftige Wertschöpfung.

Beispiel Hochwasser (vgl. Beispiel in Anh 2.5): Der vom Hochwasser betroffene Betrieb kann aufgrund der entstandenen Schäden mehrere Wochen nicht produzieren. Er muss aus diesem Grund Ertragsausfälle hinnehmen.

Je nach den Auswirkungen der Gefährdungen kann zur Abschätzung der Vermögensschäden ein unterschiedlicher Blickwinkel gewählt werden:

• Gesamtwirtschaftlich: Als Indikator für die gesamtwirtschaftliche Leistungsfähigkeit wird die Summe der inländischen Wertschöpfung verwendet. Diese wird im Bruttoinlandprodukt (BIP) quantifiziert. Eine Reduktion der wirtschaftlichen Leistungsfähigkeit entspricht also einer Abnahme des BIP.

• Individuell oder kleinräumlich: Eine Reduktion der wirtschaftlichen Leistungsfähigkeit der Betroffenen oder einer räumlich begrenzten Einheit.

A1	A2	A3	A4	A5	A6	A7	A8
≤ 5 Mio.	6–15 Mio.	> 15–50 Mio.	> 50 Mio.–150 Mio.	> 150 Mio. – 500 Mio.	> 500 Mio. – 1,5 Mrd.	> 1,5–5 Mrd.	> 5 Mrd.

Anh 2.7 – Beeinträchtigung der Lebensqualität

Beschreibung

Mit diesem Indikator wird die Beeinträchtigung der Lebensqualität beurteilt, die für die Bevölkerung aus Versorgungsengpässen und -unterbrüchen resultiert (Anmerkung: Die übrigen Auswirkungen von Ausfällen, z. B. auf die Wirtschaft oder daraus entstehende Personenschäden, werden mit den anderen Indikatoren beurteilt). Dieser Indikator umfasst den Ausfall oder eine starke Einschränkung der Versorgung der gesamten Bevölkerung respektive Teilen davon mit wichtigen Gütern oder Dienstleistungen. Nach ihrer Bedeutung werden sie in drei Gruppen eingeteilt.

Bedeutung	Güter	Dienstleistungen	Faktor
lebensnotwendig	Trinkwasser, Nahrungsmittel zur Grundversorgung, Medikamente	Medizinische Notfallversorgung, Kommunikation Einsatzkräfte	1
sehr wichtig	Strom, Heizenergie, Gas, Kleidung, Unterkunft	Ambulante und stationäre ärztliche Versorgung (ausser Notfallversorgung), ambulante Krankenpflege	0.3
wichtig	Sonstige Nahrungsmittel, Treibstoffe	Telefon, IT, TV Transport/Verkehr (Strasse, Schiene, Schifffahrt etc.)	0.1

Die Einschränkung der Versorgung wird als Produkt aus der Anzahl eingeschränkter Personen und der Dauer der Beeinträchtigung in Tagen verstanden. Es wird die effektive Dauer der Einschränkung der Versorgung über die betroffenen Personen zusammengezählt. Erfasst wird also die Dauer der tatsächlichen Einschränkung. So wird z. B. gezählt, wie lange die Stromversorgung insgesamt unterbrochen ist, also die Summe der Ausfallzeiten, und nicht, über wie viele Tage sich eine Strombewirtschaftung mit täglicher Unterbrechung von wenigen Stunden erstreck.

Wirtschaftliche Folgewirkungen erfassen die Indikatoren «Vermögensschäden und Bewältigungskosten» (Anh 2.5) und «Reduktion der wirtschaftlichen Leistungsfähigkeit» (Anh 2.6). Allfällige weitere Schäden an der Bevölkerung werden zudem mit den Indikatoren «Todesopfer», «Verletzte/Kranke» und «Unterstützungsbedürftige» bewertet (vgl. Anh 2.1–2.3)

A1	A2	A3	A4	A5	A6	A7	A8
≤ 50'000	> 50'000 – 150'000	> 150'000 – 0.5 Mio.	> 0.5 Mio. – 1.5 Mio.	> 1.5 Mio – 5 Mio.	> 5 Mio – 15 Mio.	> 15 Mio. – 50 Mio.	> 50 Mio.

Anh 2.9 – Vertrauensverlust in Staat/Institutionen

Beschreibung

Der Indikator misst die Schädigung des Vertrauens in den Staat und seine Institutionen. Die Institutionen umfassen Exekutive, Legislative, Judikative sowie staatliche oder kantonale Organisationen, wie beispielsweise Verwaltungen, Armee oder Polizei. Dazu zählen aber auch die kritischen Infrastrukturen, da die Bevölkerung erwartet, dass in der Schweiz die Verfügbarkeit von essenziellen Gütern und Dienstleistungen wie Strom, Wasser, Gas usw. nicht schwerwiegend beeinträchtigt ist.

Die Intensität des Vertrauensverlustes wird qualitativ beschrieben (vgl. Ausmassklassen).

A1	A2	A3	A4	A5	A6	A7	A8
Wenige Tage dauernde und auf Themen geringer Bedeutung bezogene Beeinträchtigung des Vertrauens (z.B. kritische Berichterstattung in Schweizer Medien)	Mehrere Tage bis wenige Wochen dauernde und auf Themen geringer Bedeutung bezogene Beeinträch-tigung des Vertrauens (z.B. kritische Berichterstattung in Schweizer Medien)	Wenige Tage dauernde und auf Themen mittlerer Bedeutung bezogene Beeinträchtigung des Vertrauens (z.B. sehr kritische Berichterstattung in Schweizer Medien)	Eine bis wenige Wochen dauernde und auf Themen mittlerer Bedeutung bezogene Schädigung des Vertrauens (z.B. sehr kritische Berichterstattung in Schweizer Medien, vereinzelte Demonstra-tionen)	Eine bis wenige Wochen dauernde und auf bedeutende Themen bezogene Schädigung des Vertrauens (z.B. extrem kritische Berichterstattung in Schweizer Medien; vereinzelte Demonstra-tionen)	Wenige bis mehrere Wochen andauernde und auf bedeutende Themen bezogene Schädigung des Vertrauens (z.B. Streiks, grössere Demonstra-tionen)	Mehrere Wochen andauernde und auf bedeutende Themen bezogene Schädigung des Vertrauens (z.B. Vielzahl von Streiks, vereinzelte Massendemonstrationen)	Mehrere Wochen andauernde, wesentliche Schädigung des allgemeinen Vertrauens (z.B. lang andauernde Streiks in vielen Bereichen, Massendemonstrationen in der gesamten Schweiz)

Anh 2.10 – Geschädigtes Ansehen im Ausland

Beschreibung

Dieser Indikator umfasst die Intensität und Dauer eines geschädigten Ansehens der Schweiz im Ausland, d. h. der Ruf der Schweiz ist beeinträchtigt und die Schweiz als Partner in bi- und multilateralen sowie internationalen Abkommen wird infrage gestellt. Der Indikator berücksichtigt die Intensität der Schädigung des Ansehens und die Dauer der Schädigung.

A1	A2	A3	A4	A5	A6	A7	A8
Einzelne Tage dauernde und auf Themen geringer Bedeutung bezogene Schädigung des Ansehens (z. B. Berichterstattung in einzelnen ausländischen Medien)	Einzelne bis mehrere Tage dauernde und auf Themen geringer Bedeutung bezogene Schädigung des Ansehens (z. B. Berichterstattung in zahlreichenausländischen Medien)	Einzelne Tage dauernde und auf Themen mittlerer Bedeutung bezogene Schädigung des Ansehens (z. B. negative Berichterstattung in einzelnen ausländischen Medien)	Einzelne bis mehrere Tage dauernde und auf Themen mittlerer Bedeutung bezogene Schädigung des Vertrauens (z.B. negative Berichterstattung in zahlreichen ausländischen Medien).	Mehrere Tage andauernde, auf Themen mit mittlerer Bedeutung bezogene Schädigung des Ansehens (z.B. sehr negative Berichterstattung in einzelnen ausländischen Medien).	Eine bis mehrere Wochen andauernde, auf Themen mittlerer Bedeutung bezogene Schädigung des Ansehens (z.B. sehr negative Berichterstattung in zahlreichen ausländischen Medien)	Mehrere Wochen andauernde Schädigung des Ansehens (z.B. negative Berichterstattung in nahezu allen relevanten Auslandsmedien).	Mehrere Wochen andauernde, schwere Schädigung des Ansehens (z.B. sehr negative Berichterstattung in nahezu allen relevanten Auslandsmedien)

Anh 2.11 – Schädigung und Verlust von Kulturgütern

Beschreibung

Der Indikator misst die Schädigung oder den Verlust von Kulturgütern der Schweiz. Schützenswerte Kulturgüter umfassen bewegliche oder unbewegliche Güter, die für das kulturelle Erbe der Völker von grosser Bedeutung sind. Beispiele dafür sind Bauwerke, Kunst, Denkmäler, archäologische Stätten, Bücher, Manuskripte, wissenschaftliche Sammlungen, Archivalien und Reproduktionen des Kulturgutes. Auch Gebäude wie Museen, Bibliotheken, Archive, Klöster sowie Orte, wo das bewegliche Kulturgut in Sicherheit gebracht werden kann, gehören dazu (vgl. dazu Haager Abkommen von 1954, Art. 1).

Es wird unterschieden zwischen Kulturgütern lokaler, regionaler (B-Objekte) und nationaler (A-Objekte) Bedeutung sowie Objekten unter «Verstärktem Schutz» (gemäss Eidgenössischer Kommission für Kulturgüterschutz).

Als «Schädigung» gelten schwere Einwirkungen auf Kulturgüter, die diese zerstören oder dazu führen, dass ein zeitlich oder finanziell hoher Aufwand erforderlich ist, damit die Kulturgüter restauriert oder wieder hergestellt werden können. «Verlust» umfasst das Entwenden (Diebstahl, Raub) sowie das irreversible Zerstören (z. B. Brand, Explosion, Wasser).

A1	A2	A3	A4	A5	A6	A7	A8
Keine Schädigung bis zur Schädigung/ Verlust einzelner Kulturgüter von lokaler Bedeutung	Schädigung/ Verlust mehrerer Kulturgüter lokaler Bedeutung	Keine Schädigung bis zu Schädigung/ Verlust einzelner Kulturgüter von regionaler Bedeutung	Schädigung/ Verlust von Kulturgüter regionaler Bedeutung oder einzelner Kulturgüter von nationaler Bedeutung	Schädigung/ Verlust mehrerer Kulturgüter regionaler und einzelner Kulturgüter von nationaler Bedeutung	Schädigung/ Verlust mehrerer Kulturgüter von nationaler Bedeutung	Schädigung/ Verlust vieler Kulturgüter von nationaler Bedeutung	Schädigung/ Verlust vieler Kulturgüter von nationaler Bedeutung und solcher unter «Verstärktem Schutz»

Anhang 3 – Indikatoren zur Beurteilung der Eintrittswahrscheinlichkeit / Plausibilität

Nachfolgend wird ein Vorschlag für Indikatoren zur Beurteilung der Eintrittswahrscheinlichkeit respektive Plausibilität der Szenarien präsentiert:[21]

W-Klasse	Beschreibung in Worten	Wahrscheinlichkeit	1 x in . . . Jahren	Häufigkeit (1/Jahr)
W 8	Tritt in der Schweiz durchschnittlich wenige Male pro Menschenleben ein.	> 30 %	< 30	$> 3*10^{-2}$
W 7	Tritt in der Schweiz im Durchschnitt etwa einmal pro Menschenleben ein.	10–30 %	30–100	$3*10^{-2}$ –10^{-2}
W 6	Hat sich in der Schweiz schon ereignet, kann aber schon mehrere Generationen zurückliegen.	3–10 %	100–300	10^{-2} –$3*10^{-3}$
W 5	Hat sich in der Schweiz vielleicht noch nicht ereignet, ist aber aus anderen Ländern bekannt.	1–3 %	300–1000	$3*10^{-3}$–10^{-3}
W 4	Es sind weltweit mehrere Ereignisse bekannt.	0.3–1 %	1000–3000	10^{-3}–$3*10^{-4}$
W 3	Weltweit sind nur wenige Ereignisse bekannt.	0.1–0.3 %	3000–10 000	$3*10^{-4}$–10^{-4}
W 2	Weltweit sind nur einzelne Ereignisse bekannt, sie sind jedoch auch in der Schweiz denkbar.	0.03–0.1 %	10 000–30 000	10^{-4}–$3*10^{-5}$
W 1	Weltweit sind – wenn überhaupt – nur einzelne Ereignisse bekannt. Ein solches Eintreten gilt selbst weltweit als sehr selten, ist jedoch auch in der Schweiz nicht völlig auszuschliessen.	< 0.03 %	> 30'000	$< 3*10^{-5}$

Vorschlag für Indikatoren zur Beurteilung der Eintrittswahrscheinlichkeit

Nach obiger Nomenklatur bezeichnet die Häufigkeit die Zahl der (erwarteten) Ereignisse pro Zeiteinheit. Typischerweise werden Häufigkeiten in Anzahl Ereignisse pro Jahr ausgewiesen (z. B. Anzahl der Lawinen in der Schweiz pro Jahr).

Wahrscheinlichkeit

Die Wahrscheinlichkeit bezieht sich auf ein mögliches Ereignis. Es geht darum, wie gross die Wahrscheinlichkeit ist, dass ein bestimmtes Ereignis wirklich eintritt. Die Wahrscheinlichkeit nimmt immer einen Wert zwischen 0 und 1 an. Gleichbedeutend ist ein Wert zwischen 0 und 100 %.

Die Häufigkeit gibt demnach die (erwartete) Anzahl Ereignisse pro Zeitperiode an, während die Wahrscheinlichkeit das mögliche Eintreten eines bestimmten Ereignisses beschreibt, wenn die Bedingungen für das Auftreten in diesem bestimmten Fall gegeben sind.

Die Wahrscheinlichkeit bzw. Häufigkeit mit der ein Gefährdungsszenario eintritt, wird bei naturbedingten und technischen Gefährdungen möglichst präzise bestimmt, beispielsweise auf der Grundlage von Statistiken oder durch Expertenschätzungen, wenn keine ausreichende Datengrundlage vorliegt.

[21] Diese Skalen basieren auf der Methode und den Arbeiten *von Katastrophen und Notlagen Schweiz* (2013).

Plausibilität

Mutwillig herbeigeführte Ereignisse, z. B. im Zusammenhang mit politischen Ereignissen, Kriminalität, Terrorismus und bewaffneten Konflikten lassen sich aufgrund sich ändernder Bedrohungslagen nicht klar mittels Häufigkeiten oder Wahrscheinlichkeiten beschreiben. Für diese Gefährdungen kann die Plausibilität des Auftretens eines solchen Ereignisses (z. B. innerhalb der nächsten zehn Jahre) abgeschätzt werden.

Analog zu den Wahrscheinlichkeits- und Häufigkeitsklassen kann den Gefährdungsszenarien eine Plausibilitätsklasse zugeordnet werden[22].

[22] Siehe: Katastrophen und Notlagen Schweiz – Methode zur Risikoanalyse, Version 1.03, 17. April 2013, S. 8 (Tabelle 3: Klassen für Plausibilität).

Anhang 4 – Grenzkosten und Aversionsfaktor

Anh 4.1 – Vorschläge für Grenzkosten

Indikator	Grenzkosten pro Einheit
Todesopfer	CHF 4 Mio.
Verletzte/Kranke	CHF 400 000
Unterstützungsbedürftige	CHF 250
Geschädigte Ökosysteme	CHF 11 500
Vermögensschäden und Bewältigungskosten	CHF 1
Reduktion der wirtschaftlichen Leistungsfähigkeit	CHF 1
Beeinträchtigung der Lebensqualität	CHF 500
Einschränkungen von Ordnung und innerer Sicherheit	CHF 300
Vertrauensverlust in Staat/Institutionen	A1: 2.5 Mio. / A2: 10 Mio. / A3: 32.5 Mio. / A4: 100 Mio. / A5: 325 Mio. / A6: 1 Mrd. / A7: 3.25 Mrd. / A8: 10 Mrd.
Geschädigtes Ansehen	A1: 2.5 Mio. / A2: 10 Mio. / A3: 32.5 Mio. / A4: 100 Mio. / A5: 325 Mio. / A6: 1 Mrd. / A7: 3.25 Mrd. / A8: 10 Mrd.
Schädigung und Verlust von Kulturgütern	A1: 2.5 Mio. / A2: 10 Mio. / A3: 32.5 Mio. / A4: 100 Mio. / A5: 325 Mio. / A6: 1 Mrd. / A7: 3.25 Mrd. / A8: 10 Mrd.

Quelle: Methode zur Risikoanalyse von Katastrophen und Notlagen für die Schweiz. Version 1.03, Stand 17. April 2013 – Tab. 5, S. 23

Anh 4.2 – Vorschlag für Aversionsfaktor

Eine gemeinsame Studie von BABS und PLANAT hat 2008 einen Aversionsfaktor φ vorgeschlagen, dem die drei Effekte zunehmender Unsicherheit zugeordnet werden:

- φ1: Unsicherheit bei der Eintrittswahrscheinlichkeitsabschätzung
- φ2: Unsicherheit bei der Schadenabschätzung
- φ3: Unsicherheit bei der intrinsischen Risikoeinstellung

Für die praktische Anwendung werden die drei Teilfaktoren einzeln bestimmt, letztlich aber wieder in einen Faktor φ zusammengefasst.

Quantifizierung des Aversionsfaktors φ

Dabei wurden zuerst die Teilfaktoren φ1 und φ2 zur Unsicherheit der Bestimmung der Eintrittswahrscheinlichkeiten *w* und des Schadensausmasses *A* abgeschätzt, unter Berücksichtigung eines Konfidenzintervalls von 95 % (ca. 2σ). Anschliessend wurden die beiden Teilfaktoren φ1 und φ2 zu einem gemeinsamen Faktor φ1+2 zusammengefasst, dessen Werte in der nachfolgenden Tabelle aufgeführt sind:

Anzahl Todesopfer	1	10	100	1'000	10'000	100'000	1'000'000
Eintretenswahrscheinlichkeit je Jahr	5.0 E+00	1.1 E-01	6.2 E-03	2.8 E-04	1.8 E-05	2.4 E-06	5.0 E-07
Faktor φ_{1+2}	1.0	1.25	1.5	1.8	2.15	2.5	2.9

Anschliessend wird der Teilfaktor φ3 abgeschätzt, bei dem es sich um die Aversion im engeren Sinne handelt. Die Frage, wie stark die Gesellschaft diesen Teileffekt berücksichtigen sollte, ist nicht objektiv zu bestimmen. Diese Festlegung wäre theoretisch z. B. von einer den Bevölkerungsschnitt repräsentierenden, gut informierten Gruppe von Personen im Sinne einer Ersatzöffentlichkeit zu treffen. Da ein solches Vorgehen sehr anspruchsvoll und aufwändig ist, wurden im Rahmen der Risikoaversionsstudie 2008 folgende Werte festgelegt:

Anzahl Todesopfer	1	10	100	1'000	10'000	100'000	1'000'000
Faktor φ_3	1.0	1.3	1.8	2.5	3.2	3.8	4.0

Die Verknüpfung der Teilfaktoren φ1+2 und φ3 erfolgt über folgende Formel:

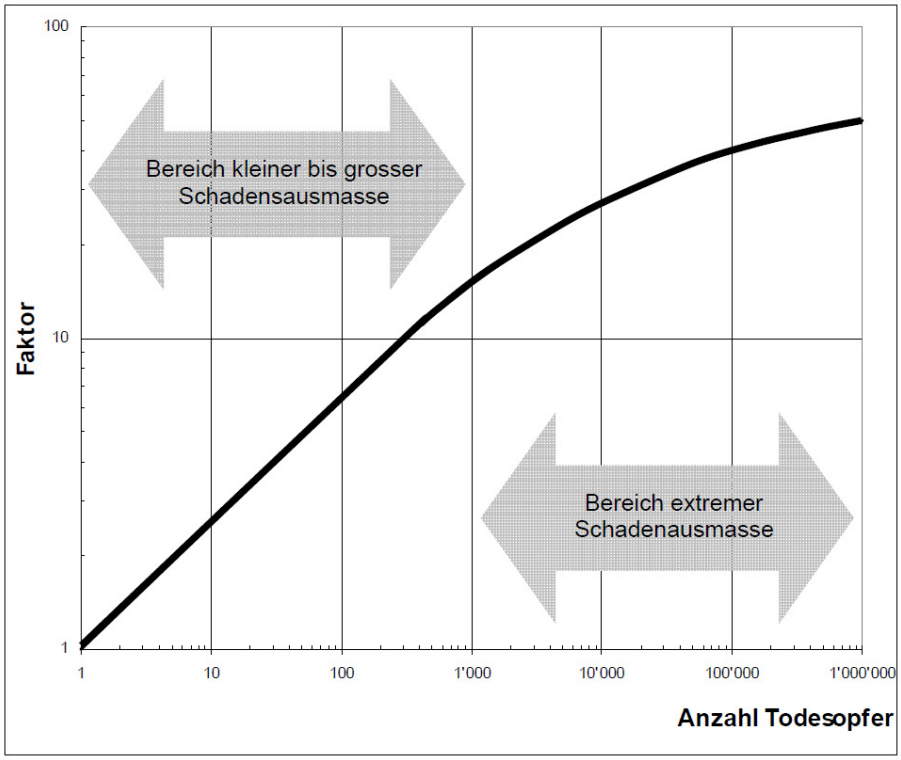
$$R_m = \sum_i w_i \cdot A_i \cdot f_i \cdot \varphi_i \cdot GK$$

wobei:

i	Szenarioindex
R_m:	Monetarisiertes Risiko aller i Szenarien
w_i :	Eintretenswahrscheinlichkeit [/ Jahr]
A_i :	Schadensausmass [Todesopfer]
f_i:	Schadenergänzungsfaktor
φ_i	$=(\varphi_{1+2}*\varphi_3)$: Aversionsfaktor
GK:	Grenzkosten

Die Gesamtwirkung dieser Faktoren ist in nachstehender Abbildung dargestellt.

Die Teilfaktoren wurden zusätzlich in einem Gesamtfaktor zusammengefasst, der mit bestehenden Aversionsfaktoren vergleichbar ist. Dabei wird zwischen zwei Bereichen bezüglich des Schadensausmasses A unterschieden: den «Bereich normaler bis grosser Schadensausmasse bis maximal 1000 Todesopfer, und den «Bereich «extremer Schadensausmasse», der von 1000 bis 1 Mio. Todesopfer reicht.



Quelle: BABS/PLANAT: Risikoaversion. Entwicklung systematischer Instrumente zur Risiko- bzw. Sicherheitsbeurteilung. Zusammenfassender Bericht. Bern, 2008, S. 13–15.

Anhang 5 – Beispiele für Schutzmassnahmen

Anh 5.1 – Beispiele baulich-technischer Massnahmen

Baulich-technische Schutzmassnahmen

Lage des Objekts

- Schutz vor Naturgefahren (Hochwasser, Erdbeben, Sturmflut, Erd- und Hangrutschungen, Lawine, Stürme etc.)
- Abstand zum Nachbargebäude
- Geschlossene Bauweise vermeiden (Zutritt über angrenzende Dächer etc. wird erschwert)
- Schutz vor technischen Gefahren (KKW-, Chemieunfälle etc.)

Bauliche Gestaltung

- Verkehrstechnische Anbindung (Notausfahrten)
- Sicherung gegen unbefugtes und gewaltsames Eindringen
- Lage der schützenswerten Gebäude
- Glatte Gebäudefassaden (keine Vorsprünge)
- Keine Aufstiegshilfen an Fassaden
- Leitungen und Versorgungsanschlüsse unterirdisch verlegt bzw. manipulationssicher
- Schaltbare Aussensteckdosen

Vorfeldsicherung

- Einzäunung (lückenlos, durchbruchsicher, Mindesthöhe, Übersteigschutz (Stacheldraht), Unterkriechschutz, videoüberwacht)
- Durchbruchsichere Türen und Tore
- Technische Zufahrtskontrollen (Gegensprechanlage, Videotechnik, Schleusenfunktion, Ausweisleser, Tastaturcodes etc.)
- Automatische elektronische Detektion (Alarmzäune, Alarmtore, Videotechnik mit Sensoren, Mauerkronensicherungen, Radarsichtstrecken, Hochfrequenzlichtschranken, Einbruchmeldetechnik)
- Aussenbeleuchtung (wenn möglich schlagschattenfrei, manipulationssicher)
- Personal zur Kontrolle der elektronischen Detektionsmittel
- Geschultes, handlungsfähiges und entsprechend ausgerüstetes Wachpersonal (z. B. mit Wärmebild-/Nachtsichtgeräten)
- Bepflanzung des Grundstückes ≠ Möglichkeit zur Überwindung der baulich-technischen Schutzmassnahmen

Gebäudesicherung

- Sichtschutz für sensible Bereiche
- Verzicht auf Lagehinweise für sensible Bereiche
- Gesonderte Sicherheitsbereiche
- Schutz der gesonderten Sicherheitsbereiche (elektronisch, mechanisch, Zutrittskontrollen, spezielle Überwachung)
- Einbruchmelder bei Türen, Fenstern, Lichtschächten
- Fenster mit Gittern
- Lichtschachtschutz (stabile Abdeckgitter, Hochhebesicherungen)
- Schutz der Ver- und Entsorgungsschächte (Gitter)
- Schutz (Gitter) von oft offenen Fenstern (z. B. in Toiletten)
- Sicherheitsglas in speziellen Sicherheitsbereichen
- Fensterschutz (einbruchhemmende Beschläge, durchwurfhemmendes Verbundsicherheitsglas, abschliessbare Fenstergriffe, verschraubte Glashalteleisten)
- Beschränkung der Anzahl Aussentüren
- Schutz des Haupteingangs: (Karten- oder Chipleser, kuppelbare/selbstverriegelnde Schlösser, elektrische Sicherheitstüröffner, automatische Türschliesser, Videogegensprechanlage, Schleuse, Trennung von Ein-und Ausgang)
- Schutz der Notausgänge (selbstverriegelnde Schlösser, automatische Türschliesser, Alarmtüren)
- Schlüsselvergabe nur an Berechtigte
- Sichere Aufbewahrung der Reserveschlüssel
- Verwaltung der Schliessberechtigungen

Brandschutz

- Blitzschutzanlagen
- Einhaltung der Brandschutzvorschriften
- Brandschutzplanung und Übungen
- Ständig besetzte Gefahrenmeldeanlage

…etc.…

Anh 5.2 – Beispiele organisatorisch-administrativer Massnahmen

Organisatorisch-administrative Schutzmassnahmen

Unternehmensintern

- Sicherheitsbeauftragter
- Betriebszugehöriges Sicherheitspersonal (Vertrautheit mit den für die Ausübung seiner Aufgaben notwendigen rechtlichen Vorschriften, den fachspezifischen Pflichten und Befugnissen sowie deren praktischen Anwendung)
- Klarheit über sicherheitsrelevante gesetzliche Anforderungen und/oder Normen
- Geregelte Sicherheitsanforderungen (z. B. durch Leitfäden, Richtlinien)
- Aufzeichnung der sicherheitsrelevanten Vorkommnisse
- Konsequenzen aus sicherheitsrelevanten Vorkommnissen
- Kenntnisse des Personals bzgl. Arbeitsschutz, Brandschutz, Erste Hilfe
- Identifikation von Gefahrenpotenzialen und Frühwarnindikatoren
- Inventar der kritischen Prozesse, Objekte, Systeme und Elemente
- Gefahrstoffkataster
- Lagepläne aller Ver- und Entsorgungsleitungen (z. B. Strom, Wasser, Gas, Telefon etc.)
- Pläne für die verschiedenen Bedrohungslagen
- Eskalationsstrategie für Sicherheitsvorfälle
- Alarmierungsplan
- Verhaltensregeln und Meldewege bei Sicherheitsvorfällen
- Belehrungen über Fluchtwege
- Evakuierungsübungen
- Übungen «Verbleiben» (z. B. bei Störfall in der Umgebung)
- Brandschutzübungen
- Einfliessen der Erkenntnisse aus den Übungen in Schulungen
- Krisenkommunikation
- Psychologische Betreuung während sicherheitsrelevanter Vorfälle

Unternehmensextern

- Notfallschaltung für Telekommunikation
- Unabhängiges integrales Sicherheitsmanagement (d. h. nur in der Hand des Betriebs)
- Vereinbarungen zwischen dem Betrieb und Sicherheitsdienstleistern (Vertragsgestaltung, praktische Zusammenarbeit, Zuständigkeiten im Krisenfall)
- Einarbeitung/Weiterbildung Sicherheitspersonal
- Kritikalitätsanalyse für Auslagerung (*Outsourcing*) von Dienstleistungen
- Vermeidung von *Open Source*-Verfügbarkeit (z. B. Luftbildaufnahmen des Betriebs im Internet etc.)

… etc. …

Anh 5.3 – Beispiele personeller Massnahmen

Personelle Schutzmassnahmen

Personal (intern und extern)

- Sicherheitsüberprüfung interner und externer Mitarbeiter
- Verpflichtung des Personals zur Einhaltung von Gesetzen, Verpflichtungen, Vorschriften, internen Regelungen etc.
- Sensibilisierung des Personals für Sicherheitsfragen (Schulungen, Übungen, Seminare, Teamtraining etc.)
- Rekrutierung (Erfahrung, Wissen, Background-Check [Strafregisterauszug etc.], Integrität, Referenzen-Check)
- Austritt (Rückgabe aller Dokumente, Büromaterial, Schlüssel, Passwörter, Badges etc., *Non-Disclosure Agreement* etc.)
- Schutz von Kader (Personenschutz etc.)

Fremdpersonen

- Anmeldung; Ein- und Austrag im Besucherjournal
- Schnelle Identifikation der Besucher (z. B. durch Besucherausweise)
- Begleitung/Beaufsichtigung der Besucher
- Anlieferer- und Warenkontrolle

… etc. …

Anh 5.4 – Beispiele organisatorisch-juristischer Massnahmen

Rechtliche Schutzmassnahmen

Verträge und Service Level Agreements bzgl.

- Lagerung von zusätzlichen Betriebsmitteln an einer anderen Lokalität
- Arrangements mit externen Dienstleistern für die Lieferung von nötigen Betriebsmitteln innerhalb kürzester Zeit
- Vereinbarte Umleitung der *just-in-time*-Lieferungen zu anderen Lokalitäten
- Lagerung von Betriebsmitteln in gesicherten Lagern bzw. Verschiffungsstandorten
- Transfer von gewissen Produktionsschritten zu anderen Lokalitäten, die nötige Betriebsmittel haben
- Vereinbarung zur Benutzung von alternativen Betriebsmitteln
- Vertragliche Übereinkünfte in Notsituationen

… etc. …

Anh 5.5 – Beispiele von Massnahmen zur Sicherstellung der Kontinuität

Massnahmen zur Sicherstellung der Kontinuität

Sicherstellung der Funktion von Schlüsselpersonen
Der Betrieb sollte angemessene Strategien für die Erhaltung von wichtigen Kenntnissen und Fähigkeiten innerhalb des Betriebs sicherstellen.

- Dokumentation über die Art der Durchführung von kritischen Prozessen und Aktivitäten
- Ein *multi-skills*Training für wichtige Mitarbeitende und Dienstleister
- Die Teilung von *core-skills*-Aktivitäten, um eine unnötige Risikokonzentration zu vermeiden
- Den Miteinbezug von Drittpersonen
- Eine geregelte Nachfolgeplanung
- Eine Wissenssicherung und ein Wissensmanagement
- Die Durchführung von Tätigkeiten im Schichtbetrieb (Business as Usual (BAU))
- Die parallele Durchführung derselben Tätigkeit auf verschiedene Standorte verteilt (BAU)
- Transfer von Tätigkeiten im Ereignisfall zu Mitarbeitenden in einer anderen Lokation

Sicherstellung von alternativen Standorten bzgl. Räumlichkeiten zur Weiterführung der Aktivitäten
Der Betrieb sollte eine klare Strategie aufzeigen, um die Auswirkungen einer Nichtverfügbarkeit einer Niederlassung bzw. einer Räumlichkeit zu verkleinern.

- Die Nutzbarkeit separater Räumlichkeiten bzw. Niederlassungen/Lokalitäten innerhalb des Betriebs
- Die Nutzbarkeit separater Räumlichkeiten bzw. Niederlassungen/Lokalitäten ausserhalb des Betriebs (z. B. bei Partnerfirmen etc.)
- Die Nutzbarkeit separater Räumlichkeiten bzw. Niederlassungen/Lokalitäten bei externen Dienstleistern
- Die Möglichkeit von Home-Office und Remote-Access-Locations (als Ergänzung zu anderen Strategien)
- Die Nutzbarkeit von anderen personellen Ressourcen in anderen Räumlichkeiten bzw. Niederlassungen/Lokalitäten.

Wiederherstellung der Einsatzfähigkeit von Technik/Technologie und Verfügbarkeit von Alternativen (insb. IKT)
Die Art der gewählten Strategien wird massgeblich von der Art der genutzten Technologien im Betrieb abhängen:

- Geografische Verteilung von technologischen Einrichtungen/Mitteln
- Die Verfügbarkeit von technologischen Einrichtungen/Mitteln als Ersatz

Zudem müssen auch für die Informationstechnologie spezifische Strategien ausgewählt werden:

- RTOs müssen identifiziert und definiert werden, v. a. für solche Aktivitäten und Prozesse, welche als kritisch eingestuft wurden
- Geografische Verteilung und Distanz zwischen technologischen Standorten
- Anzahl der technologischen Standorte
- Die Nutzung von *un-staffed-(dark)*-Standorten
- Telekommunikationsverbindungen und redundante Leitungen
- Die Art des «Failovers»: Manuelles oder automatisches Starten der redundanten Systeme oder Aktiv / Aktiv Verbindung
- Verbindungen via Drittdienstleister
- Dokumentation manueller Umgehungslösungen
- Durchführung der Aktivitäten durch Drittanbieter

Sicherstellung/Wiederherstellung von Informationen
Information, welche für die Funktionsfähigkeit des KI-Objekts essenziell ist, muss geschützt und wiederherstellbar (gemäss dem in der Analyse identifizierten Zeitrahmen) sein. Zusätzliche Information zu diesem Thema finden Sie im BS ISO/IEC 27001.

Jede Information, welche für die Funktionsfähigkeit der kritischen Prozesse und/oder des KI-Objektes erforderlich ist, muss auf folgende Punkte achten:

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Aktualität (Geltung)
- Physische Kopien
- Elektronische Kopien

Sicherstellung der Verfügbarkeit externer Dienstleistungen:
Der Betrieb sollte ein Verzeichnis mit den für die kritischen Prozesse und KI-Objekte wichtigen Betriebsmitteln erstellen. Folgendes sollte dazu berücksichtigt werden:

- Lagerung von zusätzlichen Betriebsmitteln an einer anderen Lokalität

- Arrangements mit externen Dienstleistern für die Lieferung von nötigen Betriebsmitteln innerhalb kürzester Zeit
- Vereinbarte Umleitung der *just-in-time*-Lieferungen zu anderen Lokalitäten
- Lagerung von Betriebsmitteln in gesicherten Lagern bzw. Verschiffungsstandorten
- Transfer von gewissen Produktionsschritten zu anderen Lokalitäten, die nötige Betriebsmittel haben
- Identifizierung von alternativen Betriebsmitteln
- Erhöhung der Anzahl Zulieferer (um eine Abhängigkeit von einem einzigen Zulieferer zu verringern)
- Die Förderung von BCM-Strategien bei Zulieferern
- Vertragliche Übereinkünfte in Notsituationen
- Die Identifizierung von alternativen Zulieferern
- Die Identifizierung von in- und externen Alternativlösungen
- Prüfen der BCM Lösungen von kritischen Drittanbietern

… etc. …

Anhang 6 – Integrales Schutzkonzept
Vorschlag einer Struktur für den Gesamtbericht

Zusammenfassung

1. **Einleitung**
   - Ausgangslage
   - Ziele des Berichts
   - Beteiligte Stellen

2. **Grundlagen und Vorarbeiten**
   - Allgemeine Grundlagen
   - Relevante Rechtsgrundlagen
   - Relevante Vorarbeiten

3. **Analyse**
   - Beschreibung der kritischen Infrastruktur
   - Bezeichnung der kritischen Prozesse
   - Identifikation der massgebenden Ressourcen und Verwundbarkeiten
   - Risikoanalyse
   - Allfällige Sofortmassnahmen

4. **Bewertung**
   - Bewertung gegenüber bestehenden Vorgaben
   - Priorisierung der Risiken
   - Festlegung der Grenzkosten und der Aversion
   - Quantifizierung der Risiken / Risikoübersicht

5. **(Schutz-)Massnahmen**
   - Übersicht über mögliche Massnahmen
   - Auswahl der prioritären Massnahmen und Kostenermittlung
   - Bestimmung optimale Massnahmenkombination
   - Gesamtheitliche Güterabwägung
   - Implementierung der Massnahmen (rechtlicher Anpassungsbedarf)
   - Empfehlungen für die Umsetzung (Zuständigkeiten, Vorgehen), Überprüfung und Aktualisierung
   - Festlegung des Reportings und der Überprüfung des Umsetzungsfortschritts der verschiedenen Massnahmen

6. **Weiteres Vorgehen**
   - Anträge für weiteres Vorgehen

Anhänge
- Dokumentation der kritischen Prozesse
- Liste der kontaktierten Experten und Fachstellen

Anhang 7 – Kritische Sektoren und Teilsektoren

Sektoren	Teilsektoren
Behörden	Forschung und Lehre Kulturgüter Parlament, Regierung, Justiz, Verwaltung
Energie	Erdgasversorgung Erdölversorgung Stromversorgung Fern- und Prozesswärme
Entsorgung	Abfälle Abwasser
Finanzen	Finanzdienstleistungen Versicherungsdienstleistungen
Gesundheit	Medizinische Versorgung Labordienstleistungen Chemie und Heilmittel
Information und Kommunikation	IT-Dienstleistungen Telekommunikation Medien Postdienste
Nahrung	Lebensmittelversorgung Wasserversorgung
Öffentliche Sicherheit	Armee Blaulichtorganisationen (Polizei, Feuerwehr, Sanität) Zivilschutz
Verkehr	Luftverkehr Schienenverkehr Schiffsverkehr Strassenverkehr

Quelle: Nationale Strategie zum Schutz kritischer Infrastrukturen 2018-2022, BBl **2018** 503

Anhang 8 – Koordinierende Bundesstellen

Sektor	Teilsektor	Koordinierende Bundesstellen (nicht abschliessend)*
Behörden	Forschung und Lehre	SBFI
	Kulturgüter	BABS, BAK
	Parlament, Regierung, Justiz, Verwaltung	PD, BK, EDA, Meteo-Schweiz, fedpol, IOS, NDB, EFV, ISB und LE, BAFU
Energie	Erdgasversorgung	BFE, ERI, BWL
	Erdölversorgung	BFE, ERI, BWL
	Stromversorgung	BFE, ELCOM, ESTI, ENSI, BWL
	Fern- und Prozesswärme	BFE
Entsorgung	Abfälle	BAFU
	Abwasser	BAFU
Finanzen	Finanzdienstleistungen	FINMA, EFV, SIF, BWL, BAKOM
	Versicherungsdienstleistungen	FINMA, EFV, SIF, BSV
Gesundheit	Medizinische Versorgung	KSD, BAG
	Labordienstleistungen	BAG, BLV, BABS
	Chemie und Heilmittel	BWL, Swissmedic, Armeeapotheke
Information und Kommunikation	IT-Dienst-leistungen	BWL, ISB
	Telekommunikation	BAKOM, BWL
	Medien	BAKOM
	Postdienste	BAKOM, BWL
Nahrung	Lebensmittelversorgung	BWL, BLW
	Wasserversorgung	BAFU, BWL
Öffentliche Sicherheit	Armee	Gruppe Verteidigung
	Blaulichtorganisationen (Polizei, Feuerwehr, Sanität)	fedpol, BABS
	Zivilschutz	BABS
Verkehr	Luftverkehr	BAZL, BWL
	Schienenverkehr	BAV, BWL
	Schiffsverkehr	BAV, BWL
	Strassenverkehr	ASTRA, BWL

* Die genannten Stellen legen gemeinsam mit der Geschäftsstelle SKI fest, welche weitere(n) Stelle(n) (Bund, Kantone, Verbände usw.) bei der Überprüfung und Verbesserung der Resilienz federführend und einzubeziehen sind. Geltende Kompetenzen bleiben vorbehalten.

Abkürzungen koordinierende Bundesstellen

ASTRA	Bundesamt für Strassen
BABS	Bundesamt für Bevölkerungsschutz
BAFU	Bundesamt für Umwelt
BAG	Bundesamt für Gesundheit
BAK	Bundesamt für Kultur
BAKOM	Bundesamt für Kommunikation
BAV	Bundesamt für Verkehr

BAZL	Bundesamt für Zivilluftfahrt
BBL	Bundesamt für Bauten und Logistik
BFE	Bundesamt für Energie
BLW	Bundesamt für Landwirtschaft
BSV	Bundesamt für Sozialversicherungen
BWL	Bundesamt für wirtschaftliche Landesversorgung
EDA	Eidg. Departement für auswärtige Angelegenheiten
EFV	Eidg. Finanzverwaltung
ElCom	Eidg. Elektrizitätskommission
ENSI	Eidg. Nuklearsicherheitsinspektorat
ERI	Eidg. Rohrleitungsinspektorat
ESTI	Eidg. Starkstrominspektorat
fedpol	Bundesamt für Polizei
FINMA	Eidgenössische Finanzmarktaufsicht
GS UVEK	Generalsekretariat des UVEK
IOS	Informations- und Objektsicherheit (Armeestab, VBS)
ISB	Informatik Steuerungsorgan Bund
KSD	Koordinierter Sanitätsdienst
NDB	Nachrichtendienst des Bundes
SIF	Staatssekretariat für internationale Finanzfragen
UVEK	Eidg. Departement für Umwelt, Verkehr, Energie und Kommunikation
SBFI	Staatssekretariat für Bildung, Forschung und Innovation
SNB	Schweizerische Nationalbank
VBS	Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport