Integrale Sicherheit

Umsetzung in der Praxis

Fachtagung Netzwirtschaft, 17. Juni 2014

Werner Meier, Leiter Security & BCM
Dr. Adrian Marti, Bereichsleiter Informationssicherheit AWK Group

ALPIQ

AWK GROUP
Consulting | Engineering | Project Management

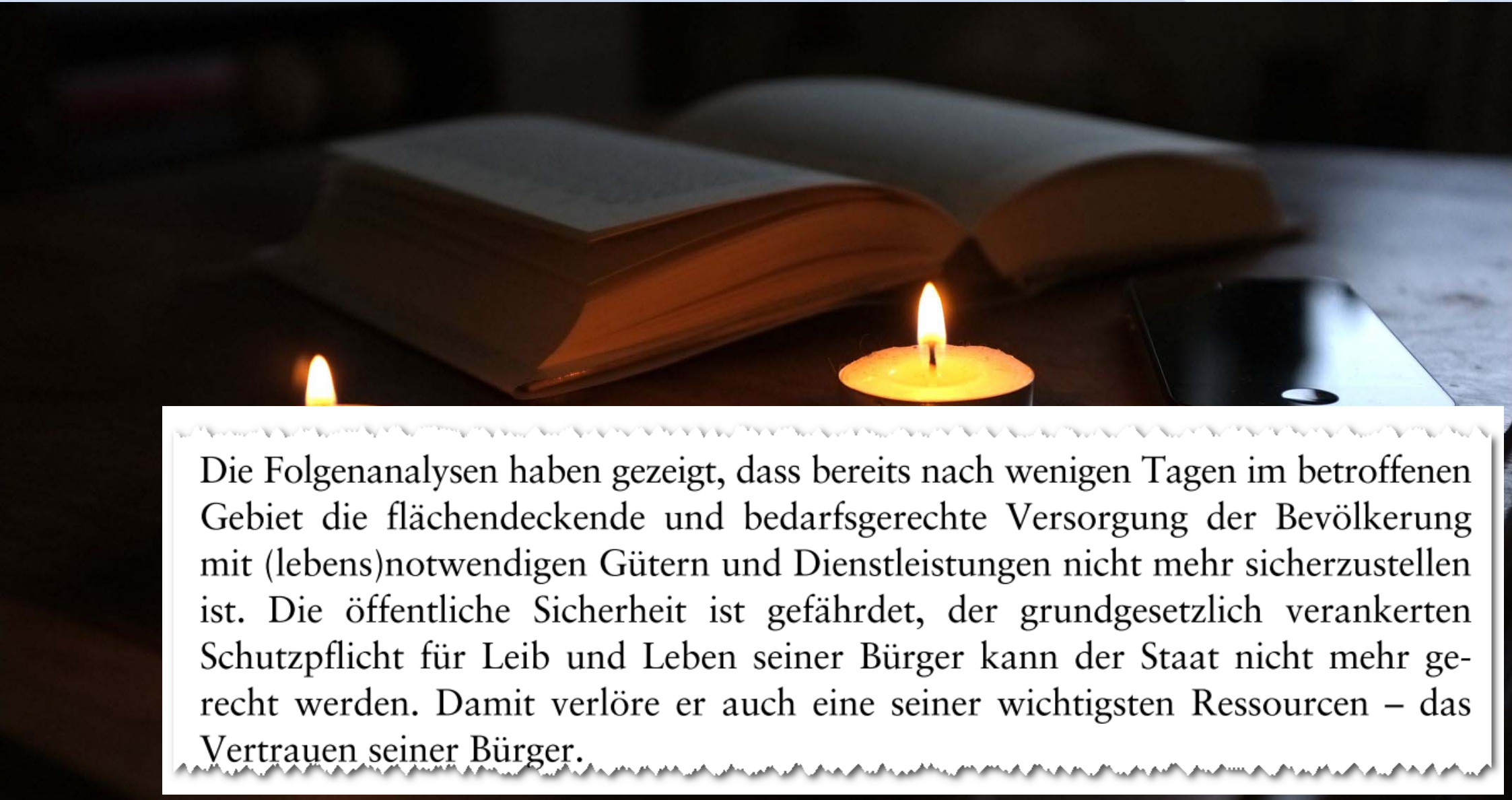
www.awk.ch

Blackout

Die Romantik …

Blackout

… währt nicht lange

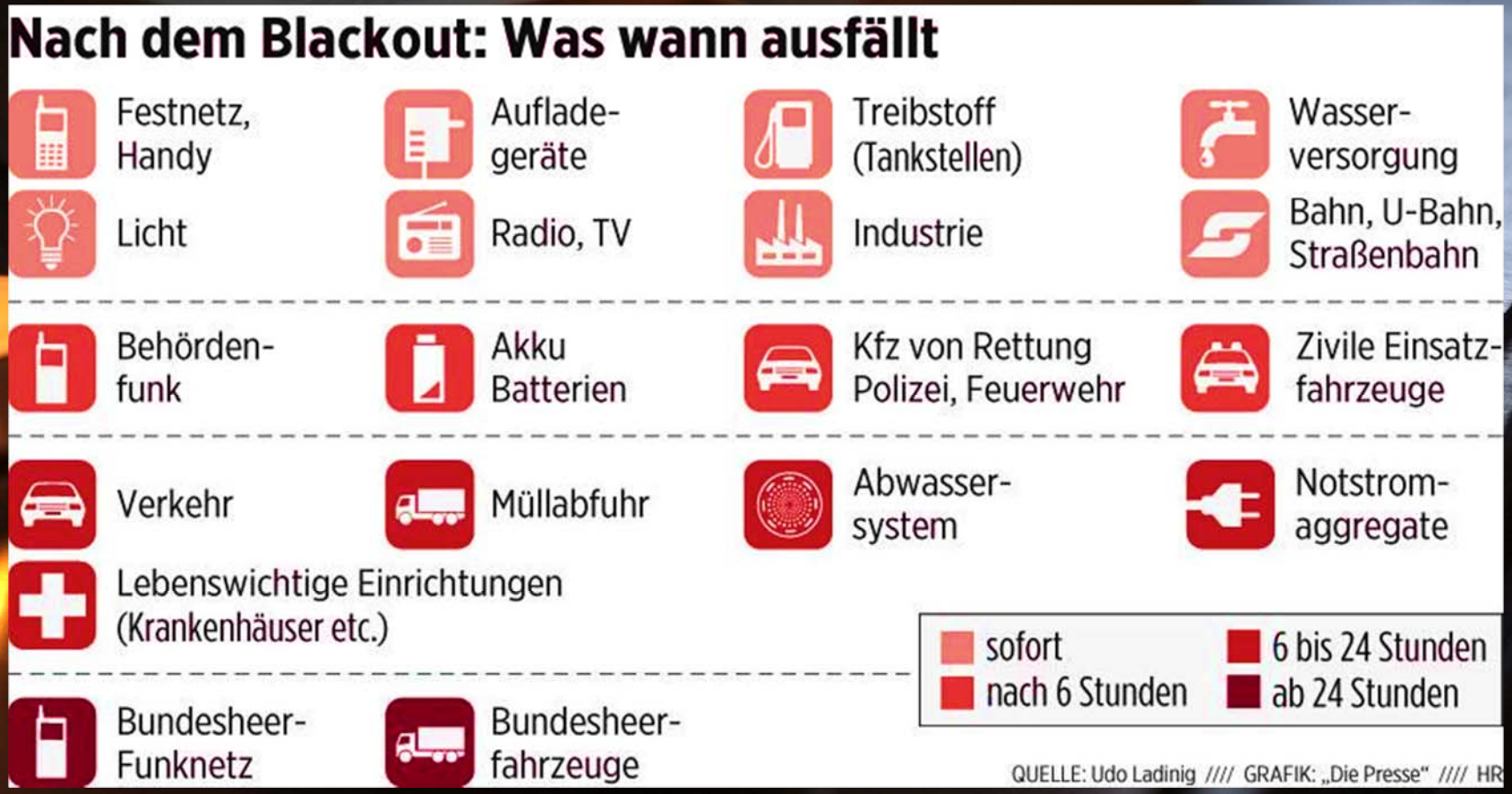


Die Folgenanalysen haben gezeigt, dass bereits nach wenigen Tagen im betroffenen Gebiet die flächendeckende und bedarfsgerechte Versorgung der Bevölkerung mit (lebens)notwendigen Gütern und Dienstleistungen nicht mehr sicherzustellen ist. Die öffentliche Sicherheit ist gefährdet, der grundgesetzlich verankerten Schutzpflicht für Leib und Leben seiner Bürger kann der Staat nicht mehr gerecht werden. Damit verlöre er auch eine seiner wichtigsten Ressourcen – das Vertrauen seiner Bürger.

- Quelle: Was bei einem Blackout geschieht: Folgen eines langandauernden und großräumigen Stromausfalls Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag – #33, 2011

Blackout

Stromausfall ist ein Paradebeispiel für »kaskadierende Schadenswirkungen«



Stärkung der Widerstandsfähigkeit

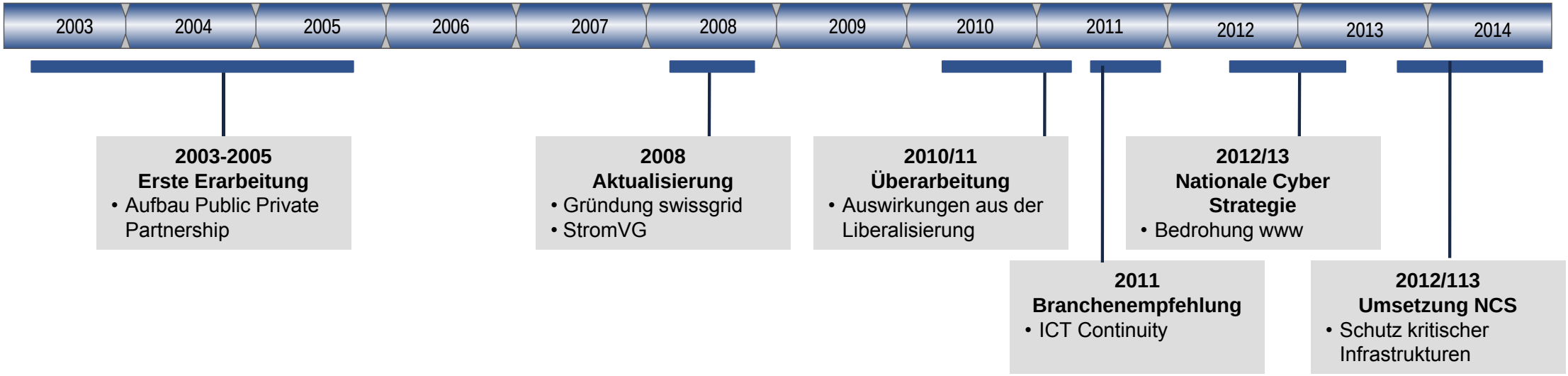
Auf nationaler Ebene: Verschiedene Partner koordinieren ihre Anstrengungen

- Die Wirtschaftliche Landesversorgung (WL) hat die Aufgabe, die aus volkswirtschaftlicher/gesellschaftlicher Sicht relevanten Sektoren einer Risikoanalyse zu unterziehen

- Betrachtete Sektoren (bisher):

Telekom	Finanzen	Gesundheits-wesen	**Energie (Elektrizität)**	Transport/ Logistik	HW/SW

- Aktivitäten im Sektor Energie (Elektrizität)



Stärkung der Widerstandsfähigkeit

Äussere Treiber

- Sektorspezifische Risikoanalyse WL ICT-I
- Branchenempfehlung VSE
- Befürchtete Aktivität des Regulators

Innere Treiber

- Unternehmenswerte
  - Wir sind ein verlässlicher Partner
  - Wir identifizieren und bewirtschaften unsere Risiken

GL Entscheid 19.4.2012

- Schaffung Konzernfunktion Group Security & BCM
- Auftrag zum Aufbau der integralen Sicherheit
  - I. Sicherheitsmanagement
    Identifikation und Bewirtschaftung der Risiken
  - II. Kontinuitätsmanagement (BCM)
    Vermeidung bzw. Beherrschung von Krisensituationen

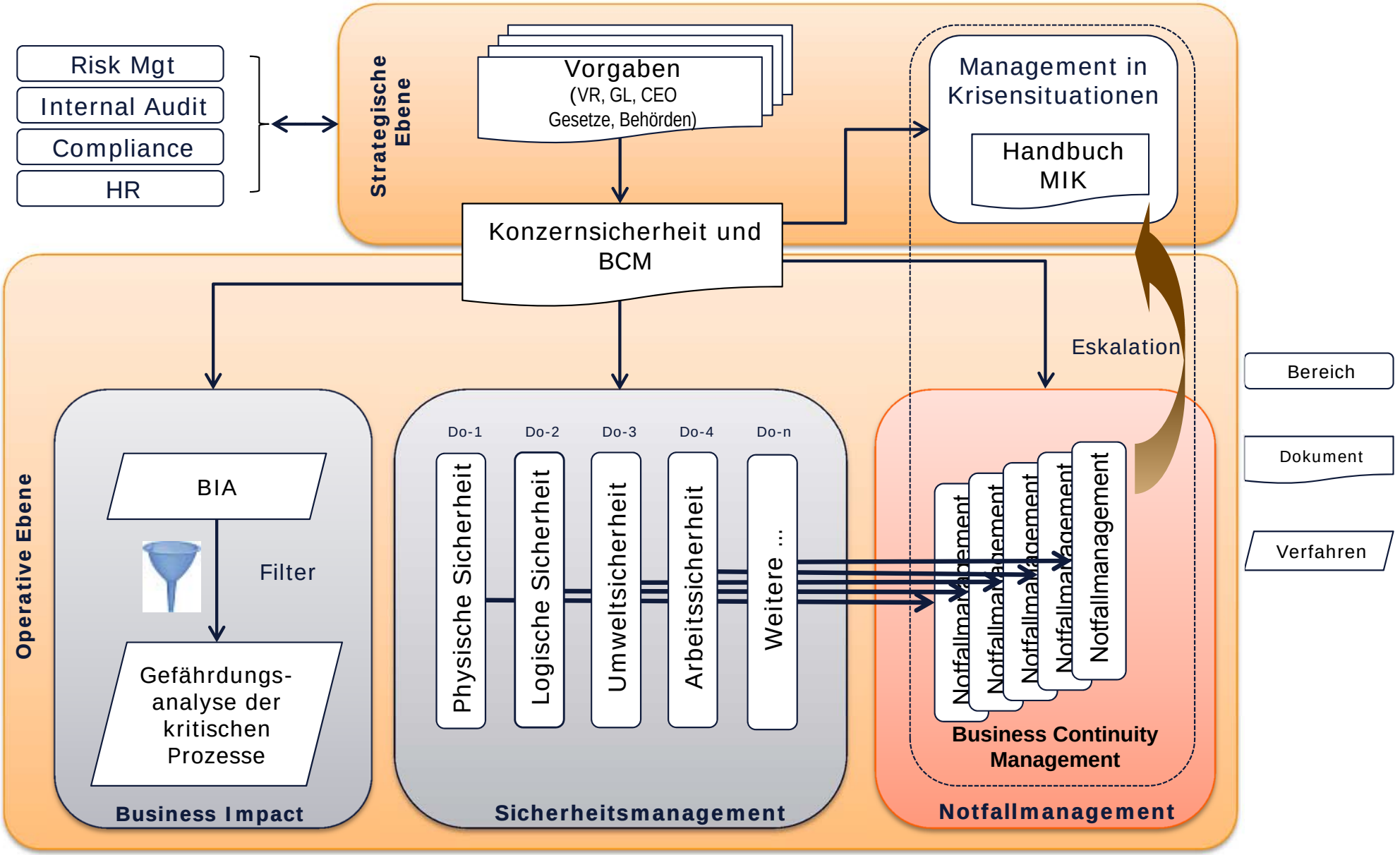
Aufbau der integralen Sicherheit

Wir orientierten uns an 7 Grundsätzen

1	**Sicherheitskultur** bewusster Umgang mit der Sicherheit
2	**Schutz der Unternehmenswerte** für die Aufrechterhaltung der Wertschöpfung und die langfristige Existenzsicherung
3	**Eigenverantwortung** Verhalten und Pflicht zur Wahrnehmung sicherheitsrelevanter Massnahmen
4	**Risikoorientierung** Systematische und verhältnismässige Behandlung der Risiken
5	**Wirtschaftlichkeit und Angemessenheit** Im Verhältnis zum möglichen Schaden
6	**Geschäftskontinuität** BCM = unternehmensweites Konzept zur Beherrschung des Restrisikos
7	**Kontinuierliche Verbesserung**

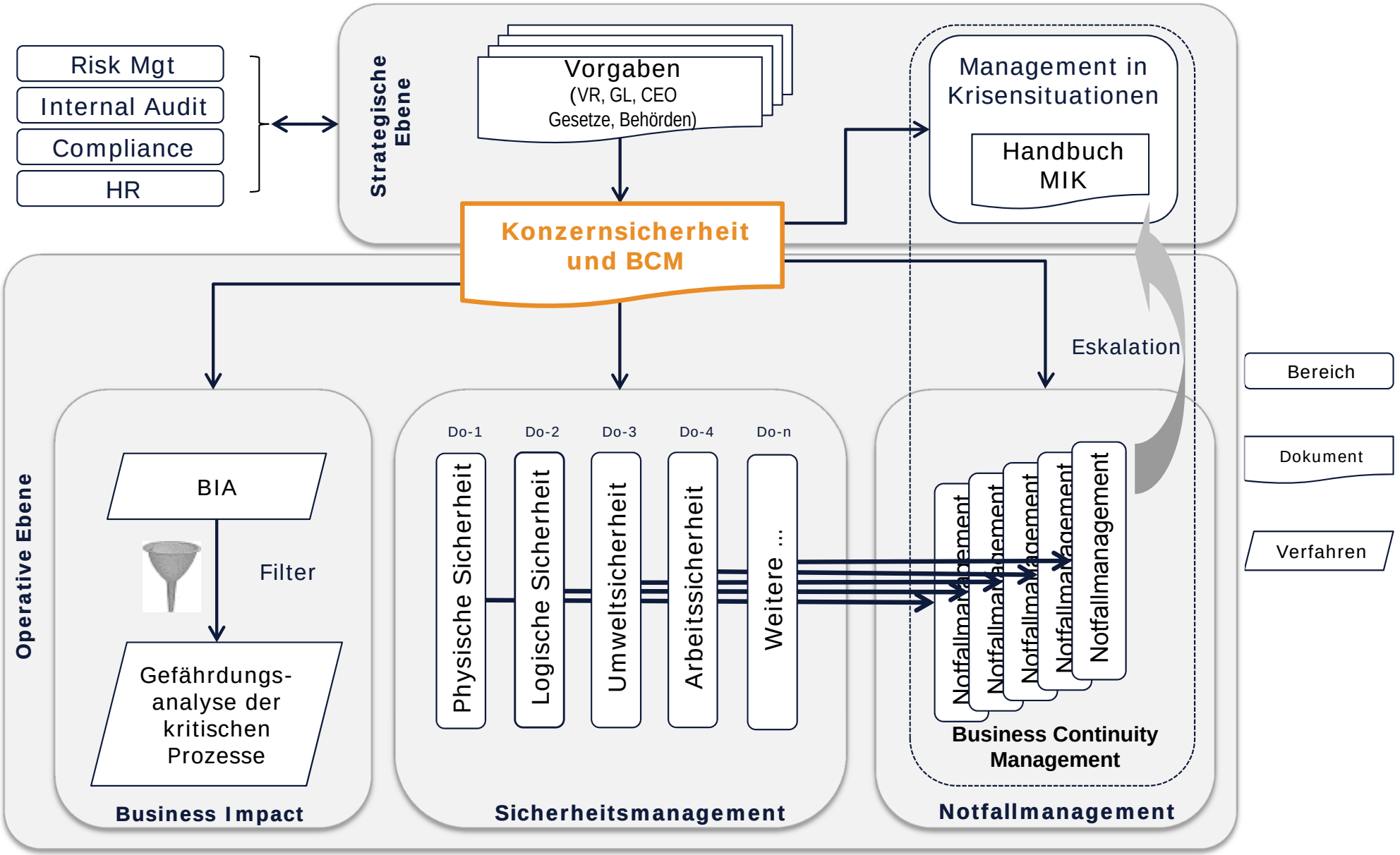
Aufbau der integralen Sicherheit

Sicherheitsdispositiv



Aufbau der integralen Sicherheit

Strategische Ebene: Konzernsicherheit und BCM



Konzernsicherheit und BCM

Zentraler Baustein zur Verankerung der integralen Sicherheit im Regelwerk der Alpiq

Führungsgrundsatz

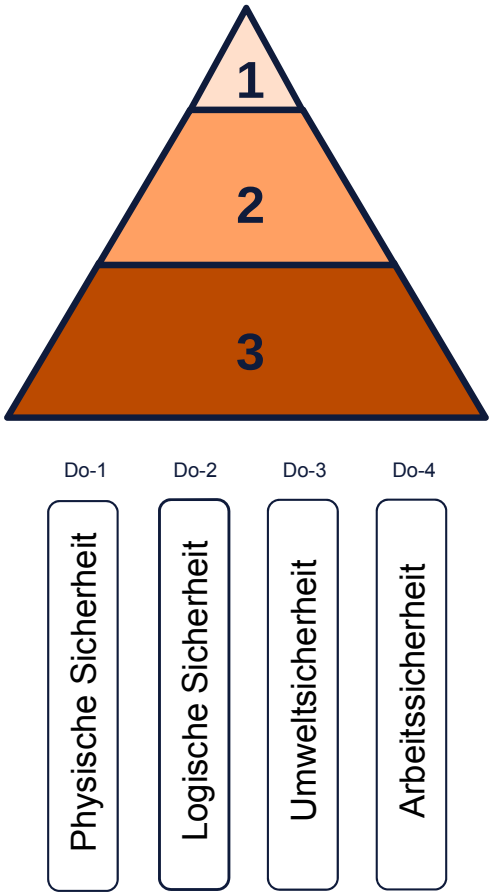
Die integrale Sicherheit ist
1. zentral gesteuert und koordiniert
2. von der Linie umgesetzt
3. von allen gelebt

Sicherheitsmanagement

- Strukturierung in zur Zeit 4 Domänen
- Je ein Fachverantwortlicher
  - Mitglied der Linienorganisation
  - Fachlich dem Leiter Security & BCM unterstellt

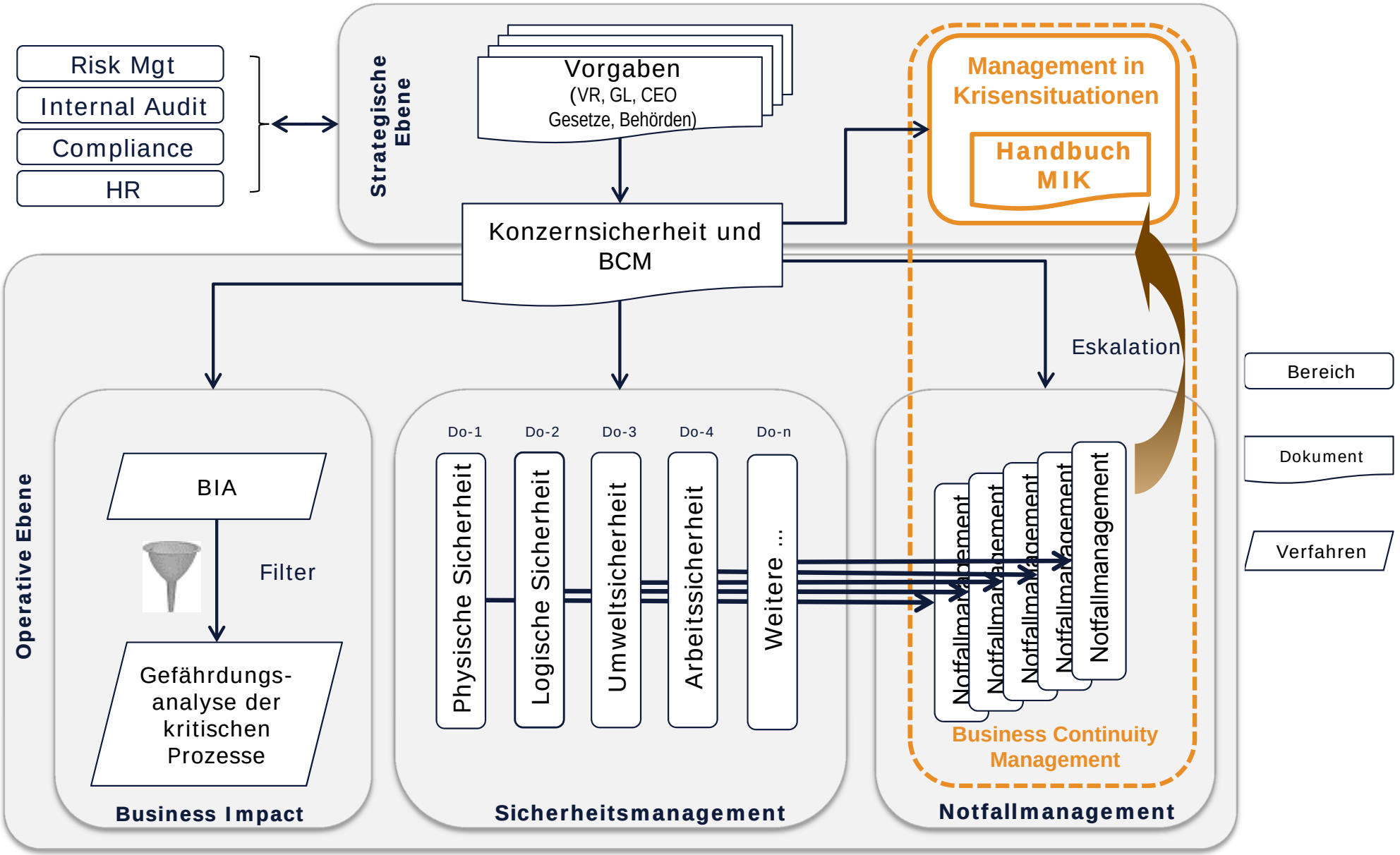
BCM

- Management in Krisensituationen (MIK)
  - Führungsstab
  - Schnittstelle zum Notfallmanagement



Aufbau der integralen Sicherheit

Business Continuity Management, Management in Krisensituationen



Business Continuity Management

Ein umfassender Ansatz zur Gewährleistung der integralen Sicherheit

BCM

- Unternehmensweiter Ansatz zur Bewältigung ausserordentlicher Ereignisse
- Stellt Erhalt / Wiederherstellung geschäftskritischer Funktionen im Ereignisfall sicher
- Erhöht die Widerstandsfähigkeit der Organisation
- Instrument zur Bewältigung von Restrisiken, welche durch das Sicherheitsmanagement nicht bewältigt werden
- MIK sichert die Führungsfähigkeit der Organisation im Ereignisfall
- Stellt mit dem Notfallmanagement die operative Ereignisbewältigung sicher

Management in Krisen MIK

Führungsinstrument des CEO zur Bewältigung von Notfall- und Krisensituationen

Notfallmanagement

Notfallorganisationen:
Auf fachtechnische Behebung spezifischer Störungen ausgerichtet

Business Continuity Management

Was wollen wir erreichen?

Management

- Bewusster Umgang mit den Restrisiken bei ausserordentlichen Ereignissen
- Bereitstellung der entsprechenden Mittel

Prozesse

- Erkennen von möglichen Schwachstellen mit Potenzial einer erheblichen Beeinträchtigung der gesamten Unternehmung
- Bewertung der entsprechenden Einflüsse auf Geschäftsprozesse & Verfügbarkeiten von Informationen und Infrastruktur
- Vorbereitung alternativer Lösungen und Wiederherstellung des Normalbetriebs

Mitarbeitende

- Sicherstellung von Schutz und Sicherheit
- Verfügbarkeit und Einsatzbereitschaft von Schlüsselpersonal
- Sicherstellung der Betreuung und der Verschiebung an alternativen Standorten

Business Continuity Management

Unser Vorgehen orientiert sich an ISO 22301 (ex BS25999)

Ziele	• Unternehmenskritische Prozesse / Funktionen und schutzbedürftige Ressourcen identifizieren • Analyse der Risiken der kritischen Prozesse • Operative Schutzziele definieren	• Definition von strategischen Schutzzielen • Abstimmung mit Geschäftsstrategie • Ableiten BCM Strategie	• Entwicklung BCP für kritische Prozesse • Definition minimaler Vorbereitungsstandard für Gesamtorganisation • Masterplan BCM Umsetzung • Erarbeitung Organisation und Rollen	▪ Ausbildung planen und durchsetzen ▪ BCP zielgruppengerecht ausgebildet und beübt ▪ Pflege und Nachführung BCP sicherstellen
Aktivitäten	➢ Unterlagen studieren ➢ Interviews	➢ Strategievarianten erarbeiten, bewerten - morphologischer Kasten - SWOT Analyse	➢ BCP operationalisieren - Ablaufpläne - Checklisten - Anpassung SLA	➢ BCM Ausbildung ➢ BCM Übungen ➢ BCP nachführen ➢ Reporting
Phase	Das Unternehmen verstehen	BCM-Strategie bestimmen	Entwicklung & Einbindung BCM-Reaktion	Übungen, Pflege und Audit
Ergebnisse	☑ Unternehmenskritische Prozesse identifiziert ☑ Kritikalität und Risiken bestimmt ☑ Bewertungsmetrik	☑ Strategische Schutzziele ☑ BCM Strategie	☑ Business Continuity Plan - Gesamtorganisation (Grundstandard) - Kritische Prozesse (detaillierter)	☑ Ausbildungskonzept ☑ Auditplanung ☑ Ausgebildete Funktionsträger ☑ Nachgeführter BCP

Was ist ein Notfall und was ist eine Krise ?

Krise

- Strategische Ebene
- Eine durch Unsicherheit gekennzeichnete Situation
- Erfordert ausserordentliche Massnahmen für die gesamte Organisation

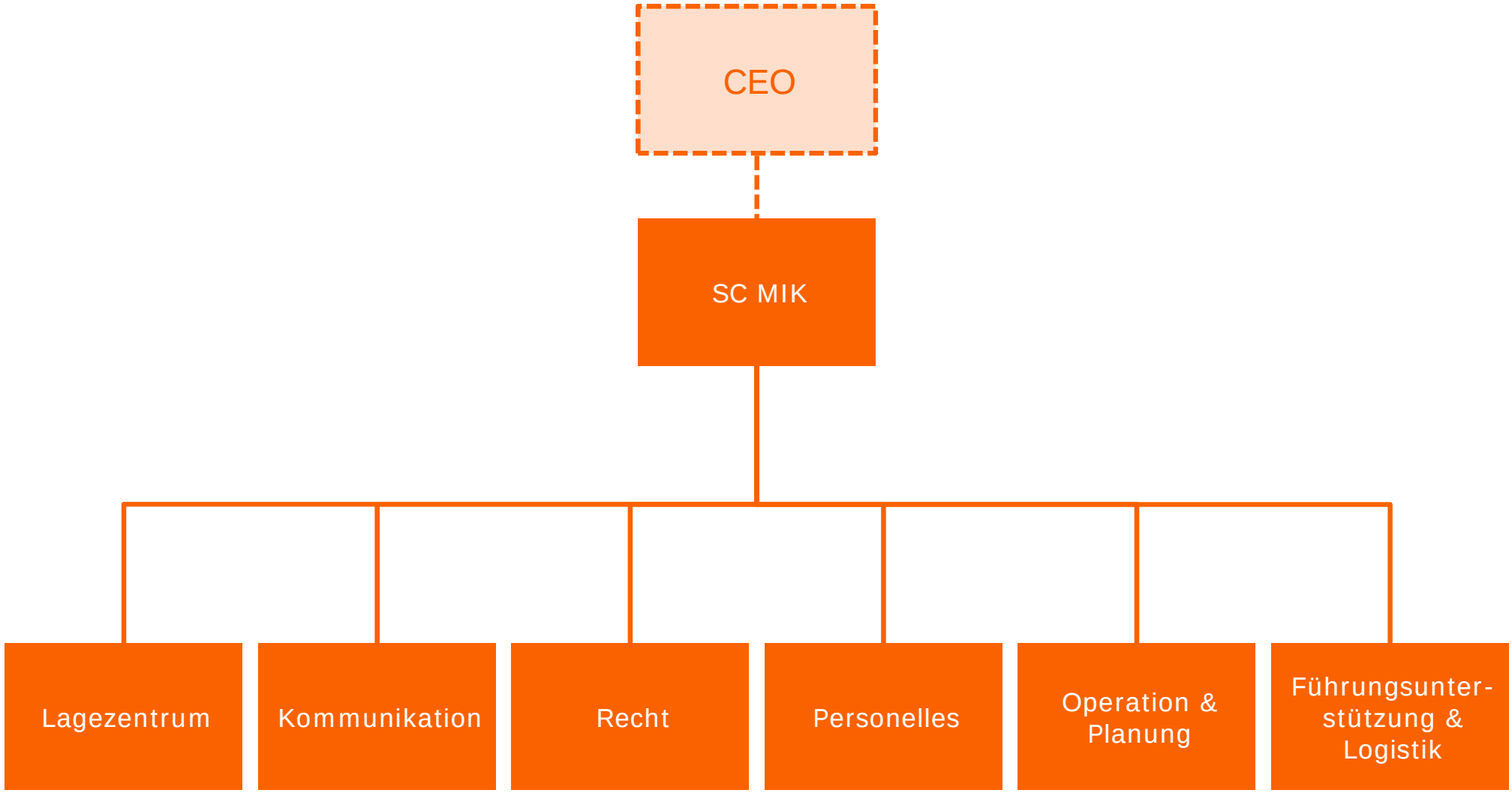
Eskalation

Notfall

- Operative Ebene
- Plötzliches und für gewöhnlich unvorhergesehenes Ereignis
- Schwerwiegende negative Folgen
- Erfordert rasches Eingreifen

Stab Management in Krisensituationen

Die Elemente des Stabs werden im Ereignisfall bedarfsgerecht aktiviert



AKV Stabschef

Für jedes Mitglied des MIK Stabs sind Aufgaben, Kompetenzen, Verantwortung beschrieben

Aufgaben

- Plant, steuert und koordiniert die Arbeit des MIK-Stabes
- Nimmt periodisch mit seinem Stab an Krisenmanagementübungen teil bzw. organisiert solche
- Berät den CEO / die Geschäftsleitung in Krisensituationen
- Unterstützt den CEO in der Kommunikation zu Gunsten des VR

Kompetenzen

- Entscheidet über die Einberufung weiterer notwendiger Mitglieder oder Experten in den Stab
- Gibt den Informationsfluss vom Krisenstab nach aussen frei
- Trifft in Abwesenheit des CEO bzw. dessen Stv. notwendige Entscheide zur Bewältigung der aktuellen Krisensituation
- Kann an Notfallübungen teilnehmen bzw. diese mit verfolgen

Verantwortung

- Ist verantwortlich für die Erstellung und Unterhalt der Führungs-Organisation, -Prozesse, -Instrumente, -Infrastruktur
- Stellt die Durchhaltefähigkeit des Krisenstabs sicher
- Stellt die nötigen Absprachen mit Polizei, Feuerwehr und weiteren externen Organisationen sicher

Szenarien Krisenmanagement

Wir nutzen Szenarien zur Plausibilisierung der Business Continuity Planung und zur Ausbildung des Krisenstabes. Reale Ereignisse können Elemente verschiedener Szenarien enthalten.

1. Nuklearereignis

2. Ausfall bzw. Fehlfunktion von Produktionsanlagen

3. Nichtverfügbarkeit von wichtigen Gebäuden

4. IT Ausfall

5. Complianceereignis

6. Grosser Personenschaden

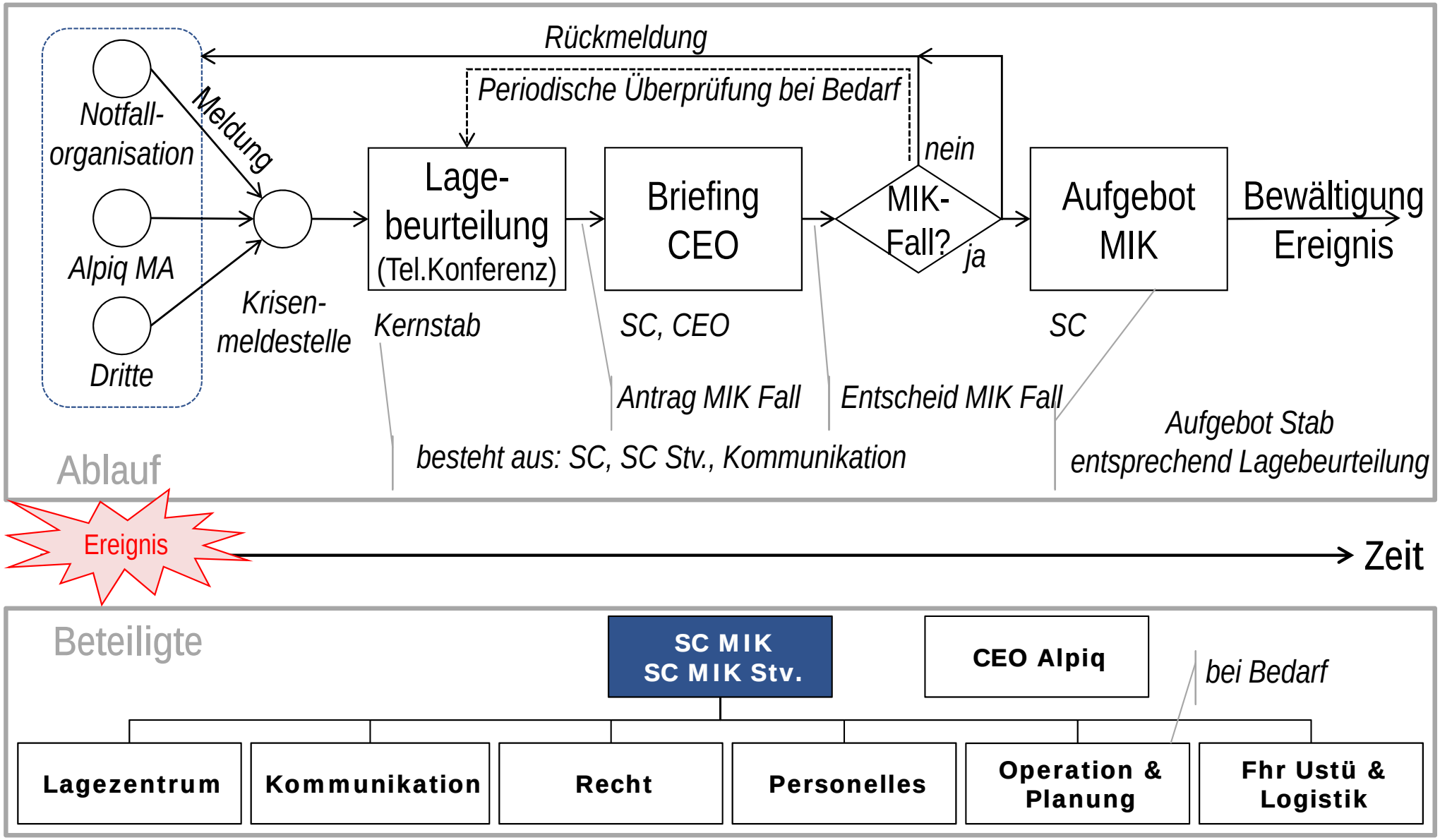
7. Zielgerichtete Gewalt

Für jedes der 7 identifizierten Szenarien sind bereitgestellt:

- Spezifische Checkliste zur Ereignisbewältigung
- Kriterien für Eskalation Notfall → Krise

Checkliste Ereignisbewältigung

MIK wird bei jedem Eintritt eines Notfalls informiert.
MIK entscheidet ob das Ereignis als Notfall oder Krise eingestuft wird.



Integrale Sicherheit

Herausforderungen

Organisation im Umbau

- Neue/angepasste geschäftskritische Prozesse als Grundlage für die Business Impact Analyse erst teilweise dokumentiert
- Verantwortlichkeiten und Zuständigkeiten im steten Wandel

Lösungsansätze

Oberstes Ziel

- Führungsfähigkeit sicherstellen
- Notfallpläne später erstellen

Business First

- Tagesgeschäft ist von höherer Dringlichkeit

Lösungsansätze

- Formale Verankerung der integralen Sicherheit im Regelwerk der Alpiq
- Persönlichen Kontakt zu den Sicherheitsverantwortlichen und Notfallmanagern suchen
- MIK Stab in praxisnaher Übung schulen

Unser Fazit
So gelingt es!

- Betten Sie ihr Krisenmanagement in ein integrales Sicherheitsdispositiv ein
  ➔ Isoliert nützt es Ihnen nichts

- Machen Sie nicht jedes Ereignis zu einer Krise
  ➔ Lassen Sie die Notfallorganisationen arbeiten

- Nachbereitung der Ereignisse ist Bestandteil der kontinuierlichen Verbesserung
  ➔ Lernen Sie aus bewältigten Ereignissen

- Nutzen und trainieren Sie eine bewährte Entscheidungsfindungsmethode
  ➔ Im Ereignisfall ist es zu spät dafür

Ihr Kontakt

Alpiq Management AG, Werner Meier
Tel. 062 286 77 70, werner.meier@alpiq.com

AWK Group AG, Dr. Adrian Marti
Tel. +41 58 411 97 67, adrian.marti@awk.ch

ALPIQ

AWK GROUP
Consulting | Engineering | Project Management