HISOLUTIONS

Gut vorbereitet durch die Krise

Know-how to go – Incident Response in der Praxis

Sophie-Louise Pries

Sophie-Louise Pries

Consultant

Fachliche Schwerpunkte:

- Schulungen und Übungen im Bereich Krisenmanagement und Krisenkommunikation
- Krisenmanagement bei Incident Response Einsätzen
- Beratung zum Thema Business Continuity Management

Background und Qualifikationen:

- Blackout Prepardness im KRITIS Umfeld
- Katastrophenschutz und öffentliche Gefahrenabwehr
- BCM Praktiker

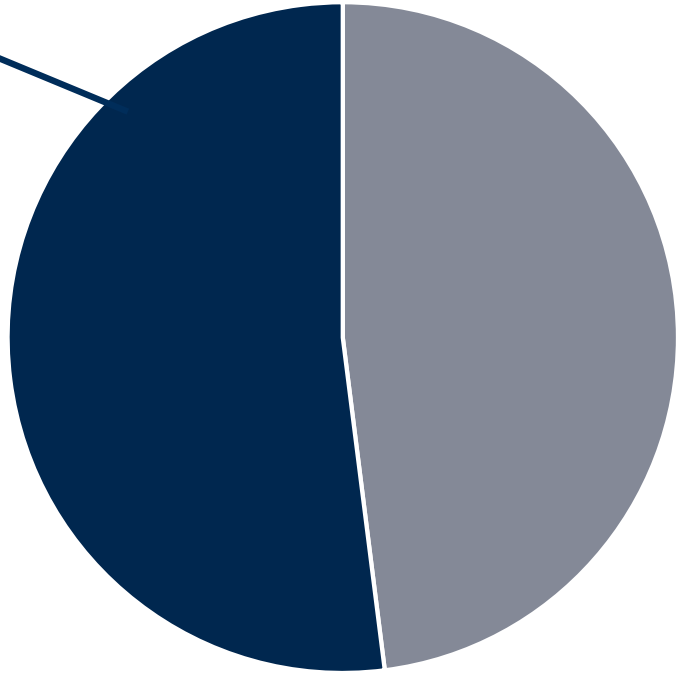
Agenda

1. Warum die richtige Vorbereitung so wichtig ist
2. Geschäftsprozesse absichern: Vorbeugen ist besser als heilen
3. Notfallstab: Im Ernstfall richtig handeln
4. Vorteile und Stolpersteine der Krisenvorbereitung

1. Warum die richtige Vorbereitung so wichtig ist

Kein Unternehmen ist sicher vor Cyberangriffen

52% aller befragten Unternehmen sehen ihre geschäftliche **Existenz durch Cyberangriffe bedroht.**



Quelle: Bitkom Studie Wirtschaftsschutz 2023 - https://www.bitkom.org/Bitkom/Publikationen/Studie-Wirtschaftsschutz

Grund 1: Statistische Wahrscheinlichkeit

- Die Weltbevölkerung wächst
- Technologie wird überall zunehmend genutzt
- Ständig zunehmende Menge von Kontakten
- Steigende Komplexität der Lieferketten durch eine steigende Anzahl an Geschäftspartnern durch Globalisierung und Outsourcing

→ Bei angenommener konstanter Fehlerquote, steigt die absolute Menge an Fehlern und Schwachstellen und in deren Folge die absolute Menge an Ausfällen.

Grund 2: Komplexität

- Der Komplexitätsgrad von Technologie steigt
- Es ist kaum noch möglich, Auswirkungen von Ausfällen innerhalb eines komplexen Systems zuverlässig vorherzusagen
- Moderne Technologie-Systeme werden als unbeherrschbar / unkontrollierbar empfunden (Industrie 4.0 Entwicklung)

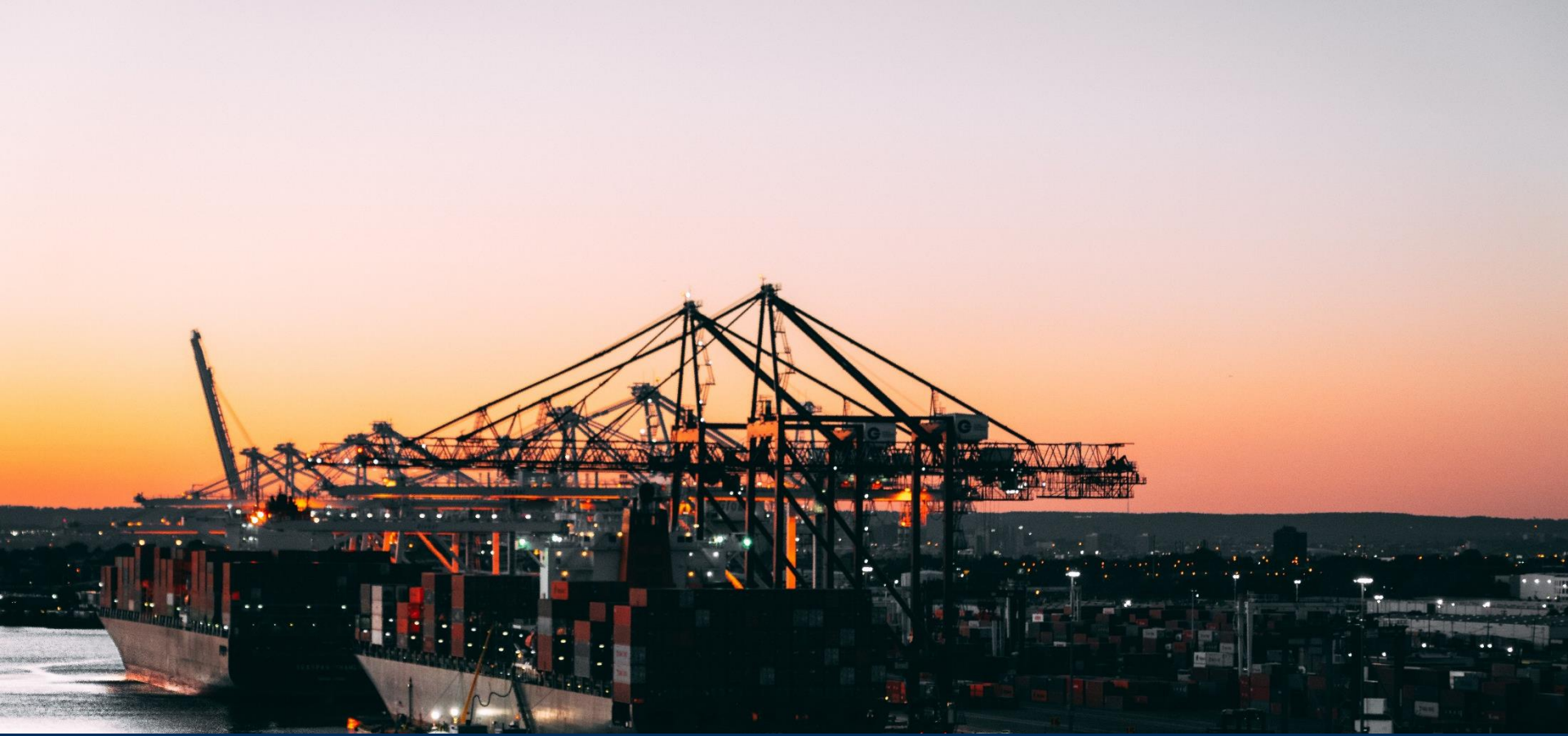
→ Technologische Fehler werden (zunehmend) zu Ausfällen an oft überraschenden Lokationen oder Einrichtungen führen.

Grund 3: Kriminalität

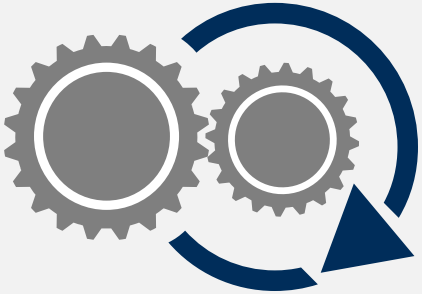
- Persönliche kriminelle Interessen: Zu persönlichen Interessen gehören Kriminalität aus finanzieller Motivation (Ransomware, Spam und Phsishing), Datenklau oder Wirtschaftsspionage und Rache.

- Politische Interessen: Kriminalität aus politischer Motivation spiegelt sich hauptsächlich in Hacktivismus oder Terrorismus wieder und soll häufig (Reputations-) schäden oder Reichweite bezwecken.

Weltweit stürzten 8,5 Mio. Microsoft Windows Systeme ab, da CrowdStrike ein fehlerhaftes Update verteilte. Die Gesamtschäden werden auf mindestens 10 Mrd. US-Dollar geschätzt. (19.07.2024)



Japans größter Hafen wurde durch einen Ransomware-Angriff für zwei Tage stillgelegt (06.07.2023)



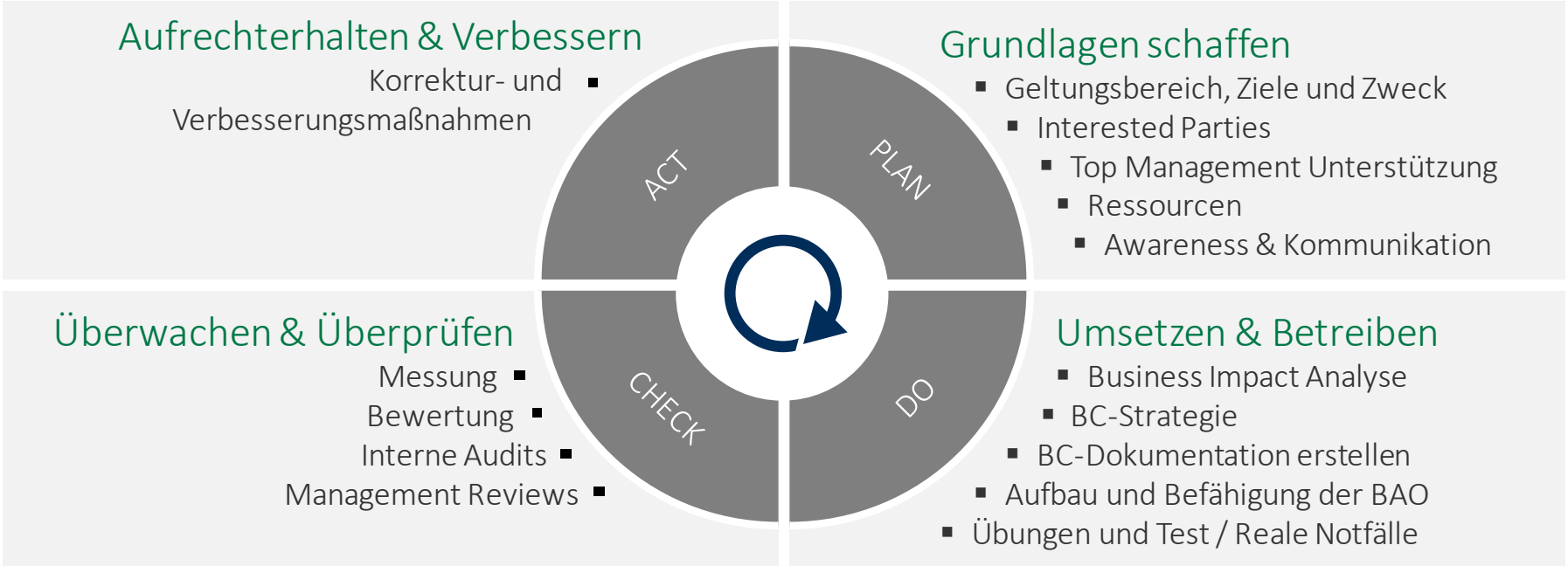
Business Continuity Management

Business Continuity Management (BCM) bezeichnet alle **organisatorischen, technischen und personellen Maßnahmen**, die **zur Fortführung des Kerngeschäfts** einer Institution nach Eintritt eines Notfalls bzw. eines Sicherheitsvorfalls dienen. Weiterhin unterstützt BCM die sukzessive Fortführung der Geschäftsprozesse bei länger anhaltenden Ausfällen oder Störungen.

Glossar BSI-Standard 200-4

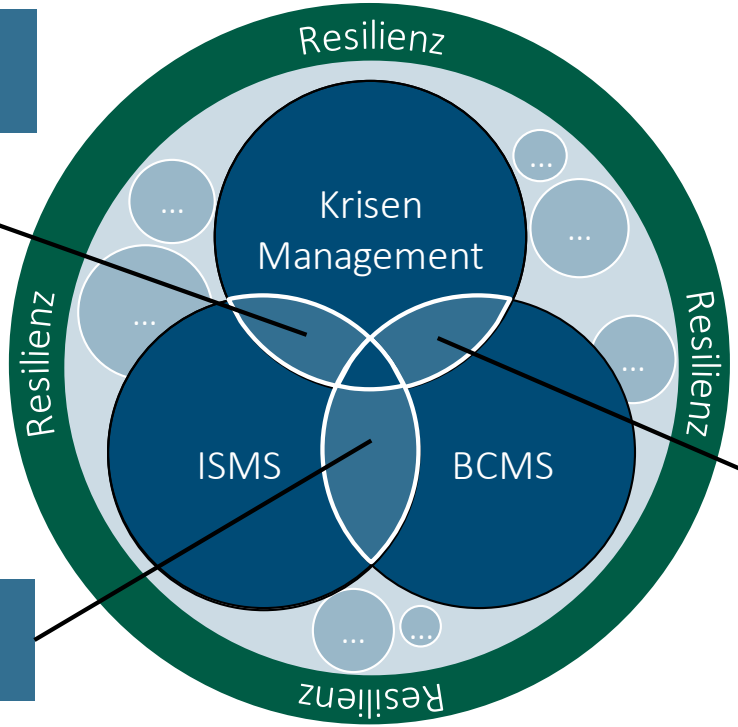
Bundesamt für Sicherheit in der Informationstechnik

Business Continuity Management hilft bei der Krisenvorbereitung



Krisen kennen keine Grenzen – Schnittstellen müssen betrachtet werden

Cyberangriffs-
/Sicherheitsvorfallbehandlung



Sicherheits- und Vorsorge-
maßnahmen (u. a. ITSCM)

Notfall-
/Krisenbewältigung

 Bildquelle: BSI-Standard 200-4

Die Umsetzung der Krisenvorbereitung besteht aus zwei elementaren Schritten

Absicherung der Geschäftsprozesse

- Business Impact Analyse durchführen
- Business-Continuity-Strategien ableiten
- Dokumentation erstellen

Aufbau und Befähigung des Notfallstabs

- Aufbau und Training des Notfallstabs
- Alarmierung und Eskalationsprozesse
- Krisenkommunikation

2. Geschäftsprozesse absichern: Vorbeugen ist besser als heilen

Geschäftsprozesse absichern: Vorbeugen ist besser als heilen

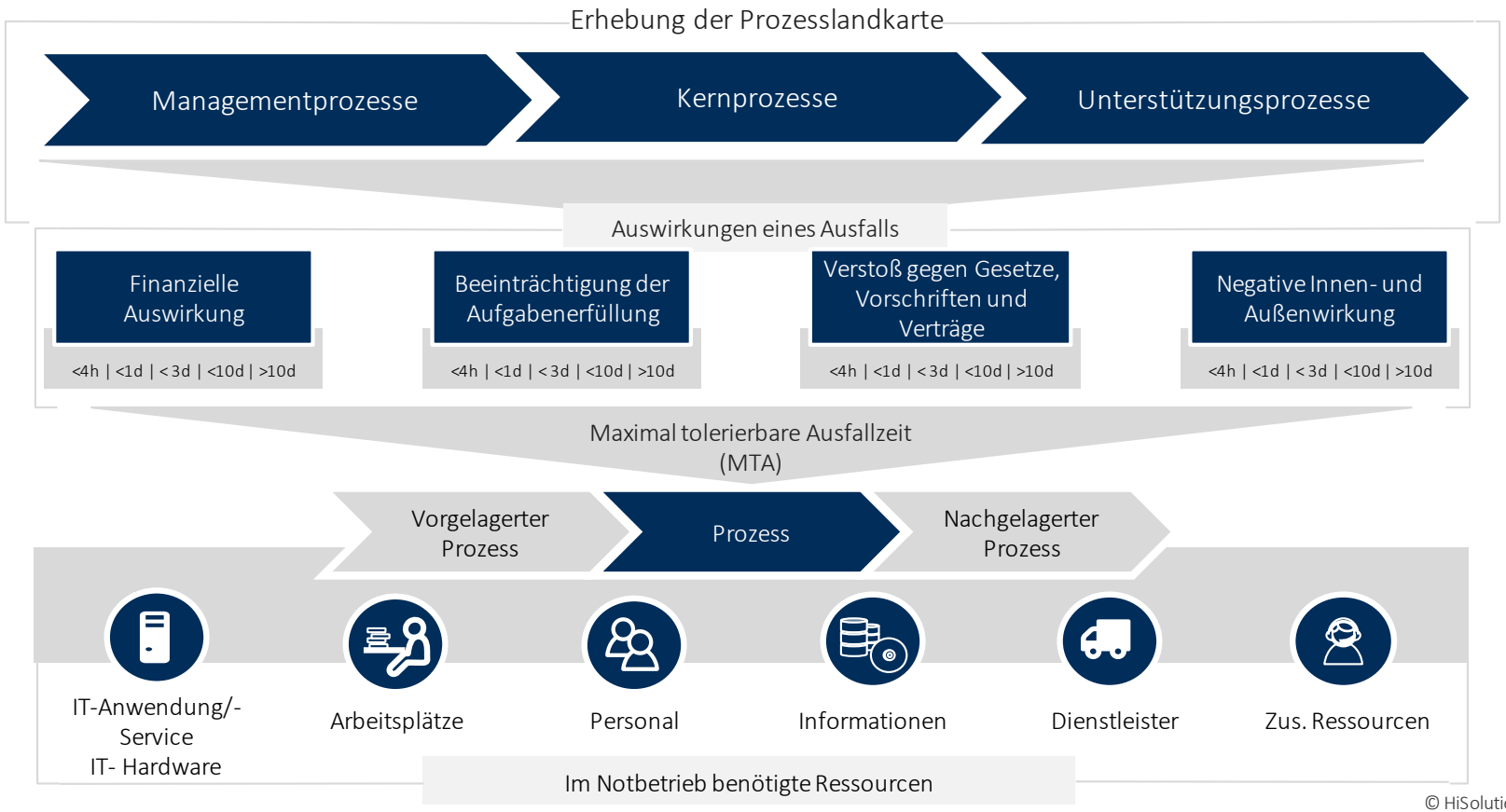
Absicherung der Geschäftsprozesse

- Business Impact Analyse durchführen
- Business-Continuity-Strategien ableiten
- Dokumentation erstellen

Aufbau und Befähigung des Notfallstabs

- Aufbau und Training des Notfallstabs
- Alarmierung und Eskalationsprozesse
- Krisenkommunikation

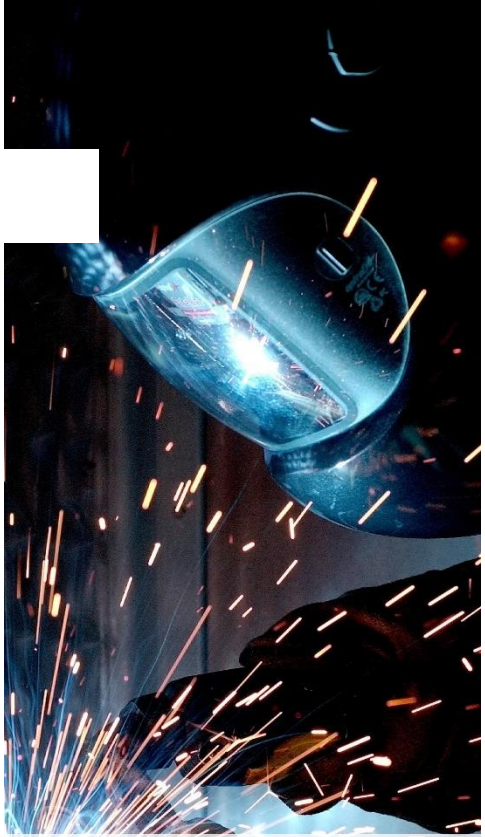
Business Impact Analyse: Identifizierung kritischer Geschäftsprozesse



Ableiten von Strategieoptionen

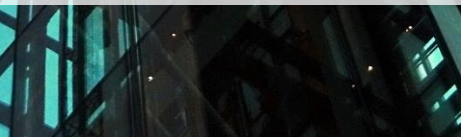
Gebäude- und Infrastrukturausfall

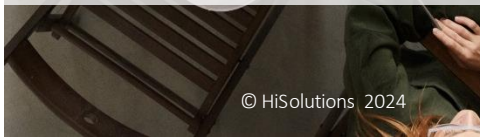
Ausfall von IT-Anwendungen



Ausfall von Dienstleistern

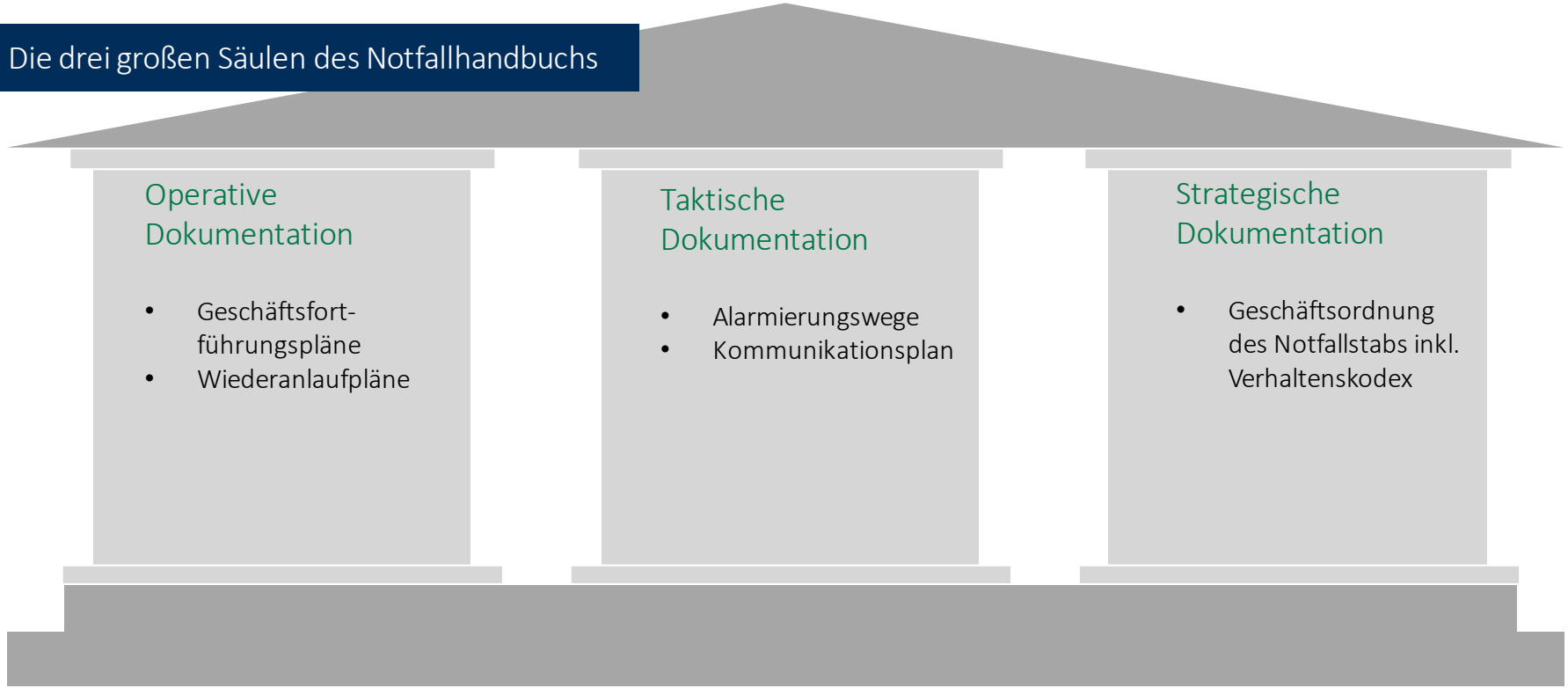
Ausfall von Personal





Notfallhandbuch

Die drei großen Säulen des Notfallhandbuchs



3. Notfallstab: Im Ernstfall richtig handeln

Notfallstab: Im Ernstfall richtig handeln

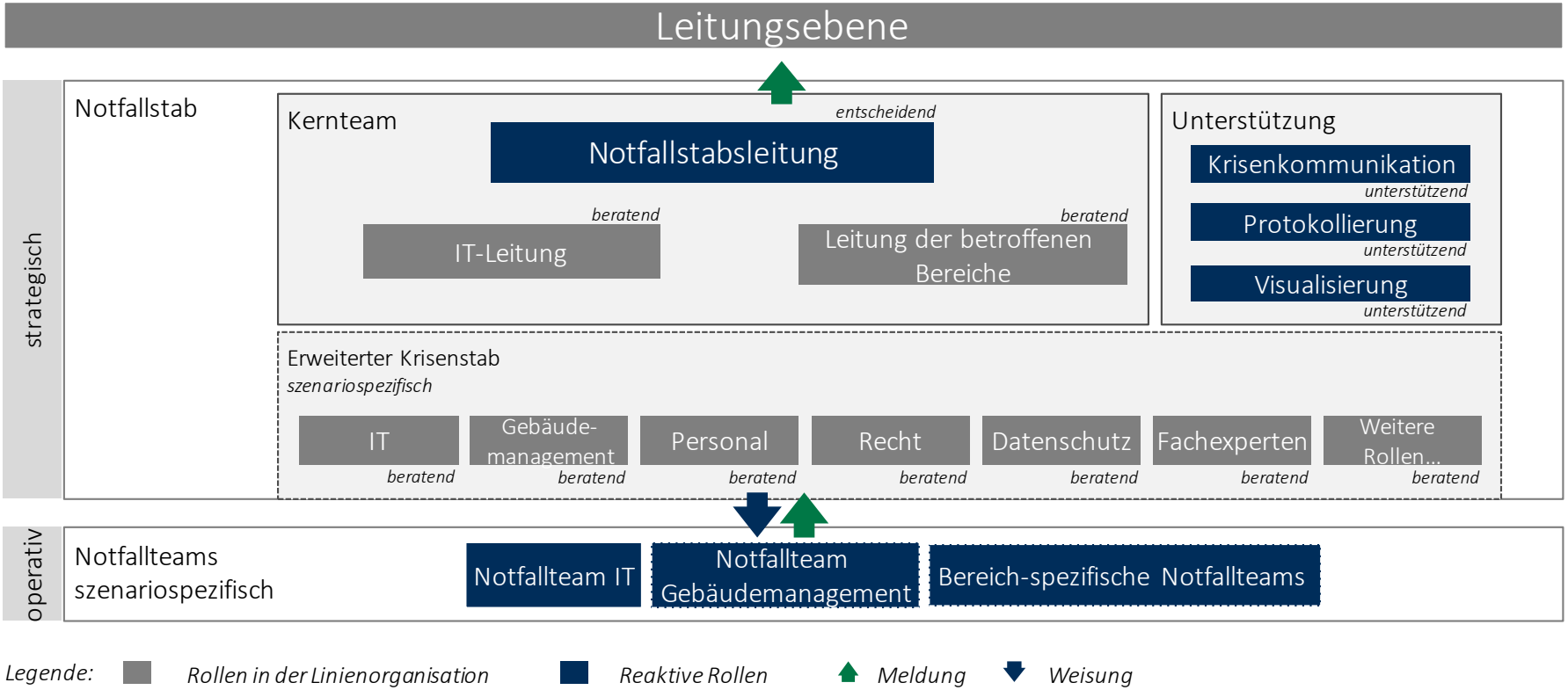
Absicherung der Geschäftsprozesse

- Business Impact Analyse durchführen
- Business-Continuity-Strategien ableiten
- Dokumentation erstellen

Aufbau und Befähigung des Notfallstabs

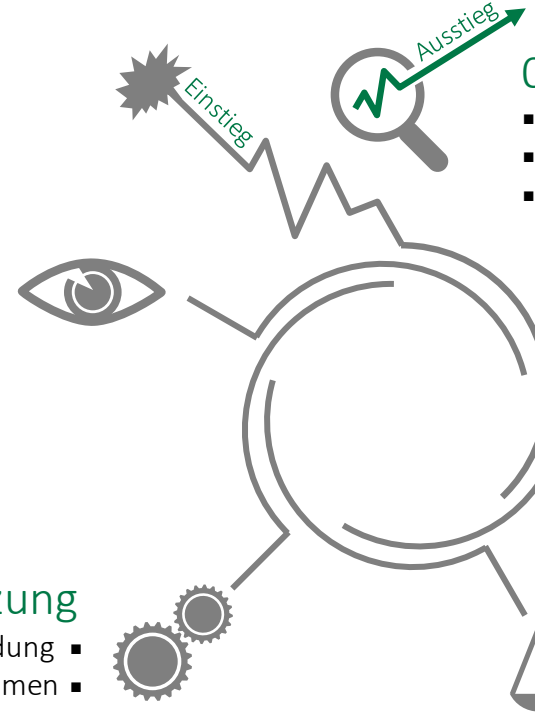
- Aufbau und Training des Notfallstabs
- Alarmierung und Eskalationsprozesse
- Krisenkommunikation

Beispielaufbau eines Notfallstabs



Legende: *Rollen in der Linienorganisation* *Reaktive Rollen* *Meldung* *Weisung*

Der Führungszyklus ermöglicht einer strukturierte Stabsarbeit



01 Lagefeststellung

- Was ist passiert?
- Wie ist es passiert?
- Welche Auswirkungen hat es?

02 Planung

- Welche Optionen stehen zur Verfügung?
- Welche Risiken haben die Optionen?
- Welchen Nutzen erreichen die Optionen?

03 Entscheidung

- Abwägen von Risiko und Nutzen
- Festlegen der Lösungsoptionen
- Leiter Notfallstab: Entscheidung treffen

04 Umsetzung

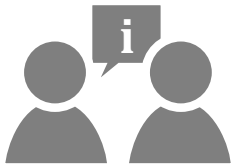
- Umsetzen der Entscheidung
- Anordnen der Maßnahmen
- Steuern der Maßnahmen

05 Kontrolle

- Beobachten der Umsetzung
- Feststellen der Wirksamkeit
- Erneute Lagebildung

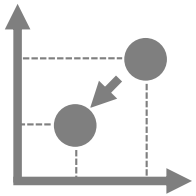
Typische Herausforderungen der Stabsarbeit

Unklare Rollen- und Aufgabenverteilung



Kommunikation im Stab

Vernachlässigte Dokumentation



Mangelnde Lagevisualisierung

Verlust der strategischen Flugebene

Feste Regeln unterstützen eine erfolgreiche Stabsarbeit

Nutzung vorliegender Pläne

Arbeits-und Besprechungsphasen (Lagebesprechungen) müssen eindeutig festgelegt und kommuniziert werden

Kurze moderierte Lagebesprechungen: Empfehlung nie länger als 30 Minuten

Regelmäßige Nutzung und Aktualisierung der Visualisierung

Klare Benennung, Terminierung und Delegierung von Aufgaben (Aufgabenmanagement)

Nutzung bspw. eines Kanban Boards zur Aufgabenvisualisierung

Fakten von Gerüchten trennen

Nachvollziehbare Protokollierung mit Angaben zu Ort, Zeit und Status

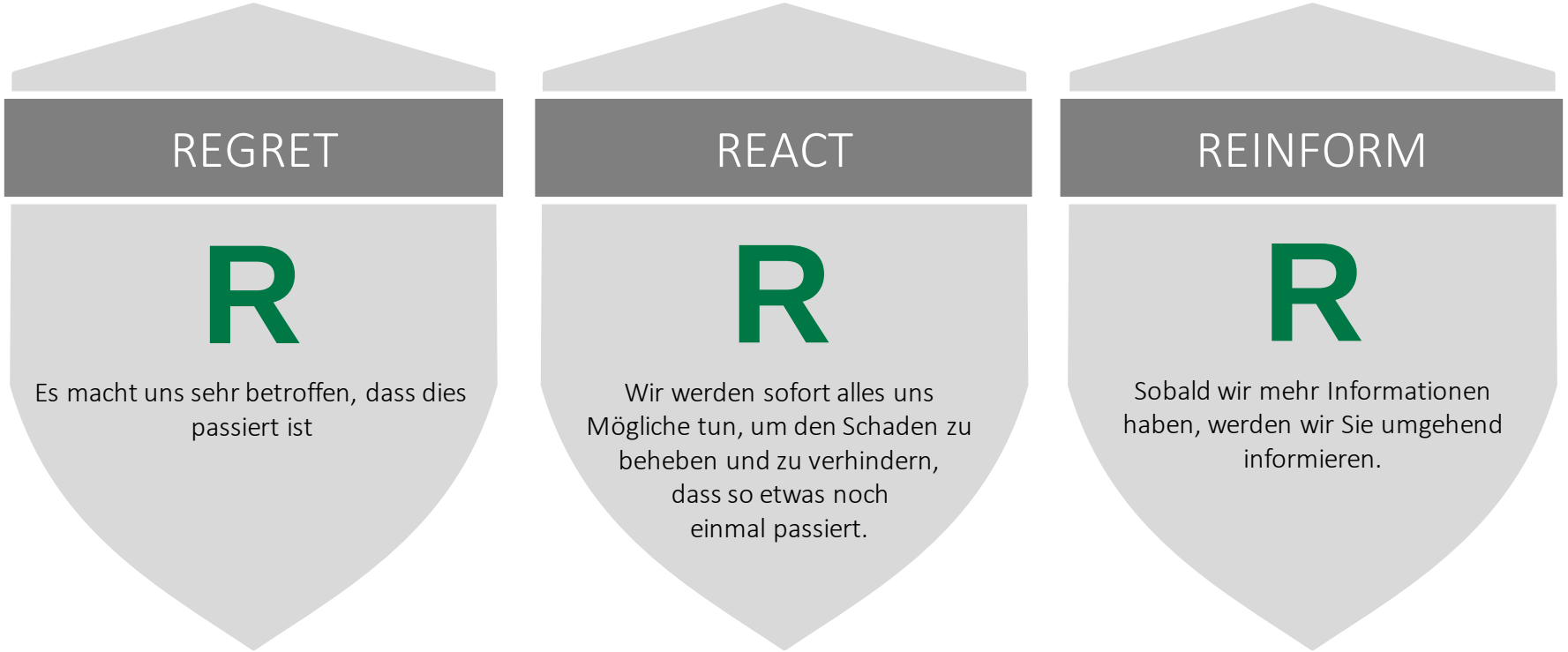
Krisenkommunikation

Wer übernimmt die Krisenkommunikation?

Ablauf der Informationswege und Umgang mit den (sozialen) Medien?

Wer sind die Interessengruppen in der Krise?

Die 3R-Regel ermöglicht eine angemessene kommunikative Erstreaktion



4. Vorteile und Stolpersteine der Krisenvorbereitung

Vorteile einer guten Krisenvorbereitung

- Reduzierung der Eintrittswahrscheinlichkeit von Schadensereignissen
- Frühzeitige Detektion und Reaktion
- Koordinierte Priorisierung der kritischen Geschäftsprozesse
- Geringere Nacharbeiten
- Frühzeitige Wiederherstellung des Normalbetriebs
- Vertrauen von externen Stakeholdern
- Einhaltung rechtlicher/vertraglicher Anforderungen

Typische Stolpersteine in der Vorbereitung auf Krisen

- Instabiles Fundament
- Mangelndes Commitment der Geschäftsführung
- Keine Awareness in der Institution
- Fehlende Wirksamkeitsprüfung

HISOLUTIONS

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com