

Physische Resilienz nach DIN SPEC 14027

Fünf typische Lücken, die Unternehmen jetzt prüfen sollten

Viele Unternehmen verfügen über einzelne Sicherheitsmaßnahmen und Krisenprozesse. Was fehlt, ist oft ein integriertes Modell, mit dem physische Resilienz systematisch bewertet, gesteuert und verbessert wird. Die DIN SPEC 14027 bietet dafür einen Orientierungsrahmen. Diese Checkliste ersetzt keine Analyse — sie hilft, typische Lücken früh zu erkennen.

BEWERTUNG

☐

Trifft zu

☐

Teilweise

☐

Nicht geklärt

1 Regelung der Verantwortlichkeiten

Physische Resilienz berührt Geschäftsführung, Standortleitung, BCM, Operations, HR, Compliance, Einkauf, IT und Krisenmanagement. Die Lücke entsteht, wenn viele beteiligt sind, aber niemand den Gesamtzusammenhang steuert.

	TRIFFT ZU	TEILWEISE	NICHT GEKLÄRT
Es ist klar definiert, wer physische Resilienz fachlich verantwortet.	☐	☐	☐
Rollen, Eskalationswege und Entscheidungsbefugnisse sind dokumentiert.	☐	☐	☐
Standort-, Bereichs- und Konzernverantwortung greifen nachvollziehbar ineinander.	☐	☐	☐
Die Geschäftsführung erhält regelmäßig ein belastbares Lagebild zur physischen Resilienz.	☐	☐	☐

Erkennbar an: Im Ereignisfall wird zunächst diskutiert, wer zuständig ist, statt auf vorbereitete Rollen und Entscheidungswege zurückzugreifen.

2 Bewertung der Standort- und Funktionsrisiken

Viele Analysen betrachten einzelne Gefahren oder Standorte — aber nicht, welche physischen Ereignisse kritische Funktionen, Lieferfähigkeit oder Entscheidungen treffen. Besonders kritisch, wenn Bewertungen veraltet sind.

	TRIFFT ZU	TEILWEISE	NICHT GEKLÄRT
Kritische Standorte, Prozesse, Funktionen und Abhängigkeiten sind identifiziert.	☐	☐	☐
Physische Bedrohungen und Verwundbarkeiten werden regelmäßig bewertet.	☐	☐	☐
Veränderungen wie neue Standorte, Lieferketten oder geopolitische Risiken fließen ein.	☐	☐	☐
Es ist nachvollziehbar, welche physischen Risiken geschäftskritische Auswirkungen haben.	☐	☐	☐

Erkennbar an: Schutzmaßnahmen orientieren sich an historischen Annahmen, nicht an aktuellen Abhängigkeiten und geschäftskritischen Funktionen.

3 Integriertes Maßnahmenmodell

Einzelmaßnahmen wie Zutrittskontrolle, Sicherheitsdienst oder Notfallplanung wirken nur begrenzt, wenn sie nicht priorisiert, aufeinander abgestimmt und mit übergeordneten Resilienzzielen verbunden sind.

	TRIFFT ZU	TEILWEISE	NICHT GEKLÄRT
Bestehende Sicherheits- und Resilienzmaßnahmen sind vollständig erfasst.	☐	☐	☐
Maßnahmen sind nach Kritikalität, Risiko und Wirkung priorisiert.	☐	☐	☐
Es gibt ein gemeinsames Zielbild für physische Resilienz.	☐	☐	☐
Investitionen in Schutzmaßnahmen werden nachvollziehbar begründet und gesteuert.	☐	☐	☐
Maßnahmen werden regelmäßig überprüft und weiterentwickelt.	☐	☐	☐

Erkennbar an: Es gibt viele Aktivitäten, aber keine klare Antwort, welche Maßnahmen für welche kritischen Funktionen am wichtigsten sind.

4 Übung und Training für Krisenroutinen

Pläne sind nur so belastbar wie ihre praktische Anwendung. Oft existieren Krisendokumente, werden aber selten realitätsnah geübt – Schwächen in Kommunikation, Entscheidung, Lagebild und Eskalation bleiben unentdeckt.

	TRIFFT ZU	TEILWEISE	NICHT GEKLÄRT
Relevante Szenarien physischer Störungen werden regelmäßig geübt.	☐	☐	☐
Krisenstäbe, Standortleitungen und Fachbereiche kennen ihre Rollen.	☐	☐	☐
Kommunikations- und Eskalationswege wurden praktisch getestet.	☐	☐	☐
Erkenntnisse aus Übungen und Vorfällen führen zu konkreten Verbesserungen.	☐	☐	☐
Es gibt belastbare Routinen für Lagebild, Entscheidung und Nachsteuerung.	☐	☐	☐

Erkennbar an: Im Ernstfall funktionieren einzelne Personen gut, aber das System hängt stark von Erfahrung, Improvisation und informellen Kontakten ab.

5 Vernetzung von Fachbereichen

Resilienz entsteht im Zusammenspiel von Corporate Security, BCM, Risk Management, HR, Operations, Compliance, Einkauf, Kommunikation und Management. Typische Schwachstelle: die Trennung von Sicherheits-, Kontinuitäts- und Managementprozessen.

	TRIFFT ZU	TEILWEISE	NICHT GEKLÄRT
Corporate Security, BCM, Risk Management und Operations arbeiten strukturiert zusammen.	☐	☐	☐
Sicherheitsrelevante Erkenntnisse fließen in Managemententscheidungen ein.	☐	☐	☐
Physische Resilienz ist mit Krisenmanagement, Business Continuity und Compliance verbunden.	☐	☐	☐
Schnittstellen zu HR, Kommunikation, Einkauf und Standortmanagement sind definiert.	☐	☐	☐
Es gibt regelmäßige Abstimmungen zu Risiken, Maßnahmen und Verbesserungen.	☐	☐	☐

Erkennbar an: Jeder Bereich hat eigene Pläne, aber es fehlt ein gemeinsames Verständnis, wie das Unternehmen als Ganzes resilient bleibt.

KURZE SELBSTEINSCHÄTZUNG

Überwiegend „Trifft zu“

Gute Basis. Prüfen Sie, ob die Strukturen vollständig, aktuell und an der DIN SPEC 14027 ausgerichtet sind.

Viele „Teilweise“

Erkennbarer Handlungsbedarf. Maßnahmen vorhanden, aber Verantwortlichkeiten, Prioritäten und Schnittstellen noch nicht systematisiert.

Viele „Nicht geklärt“

Strukturelles Risiko. Eine vertiefende Analyse bestimmt Lücken, Verantwortlichkeiten und priorisierte Maßnahmen belastbar.

MANAGEMENT-FRAGE

Könnten Sie morgen nachvollziehbar erklären, wie Ihr Unternehmen seine physische Resilienz systematisch bewertet, steuert und verbessert?

NÄCHSTER SINNVOLLER SCHRITT

Die Continuitylab GmbH unterstützt Unternehmen dabei, physische Resilienz nach DIN SPEC 14027 pragmatisch einzuordnen und weiterzuentwickeln. Für den Einstieg eignen sich:

30-Minuten-Check

Schnelle erste Standortbestimmung.

Executive Briefing

DIN SPEC 14027 für die Führung eingeordnet.

Readiness-Assessment

Strukturierte Bewertung & Roadmap.

Darauf aufbauend lässt sich ein Workshop zur physischen Resilienz durchführen, um Handlungsfelder, Prioritäten und nächste Schritte gemeinsam zu konkretisieren.

Resilienz strukturiert bewerten — und gezielt verbessern.

Erstgespräch vereinbaren →