Whitepaper
Organisational Resilience Management

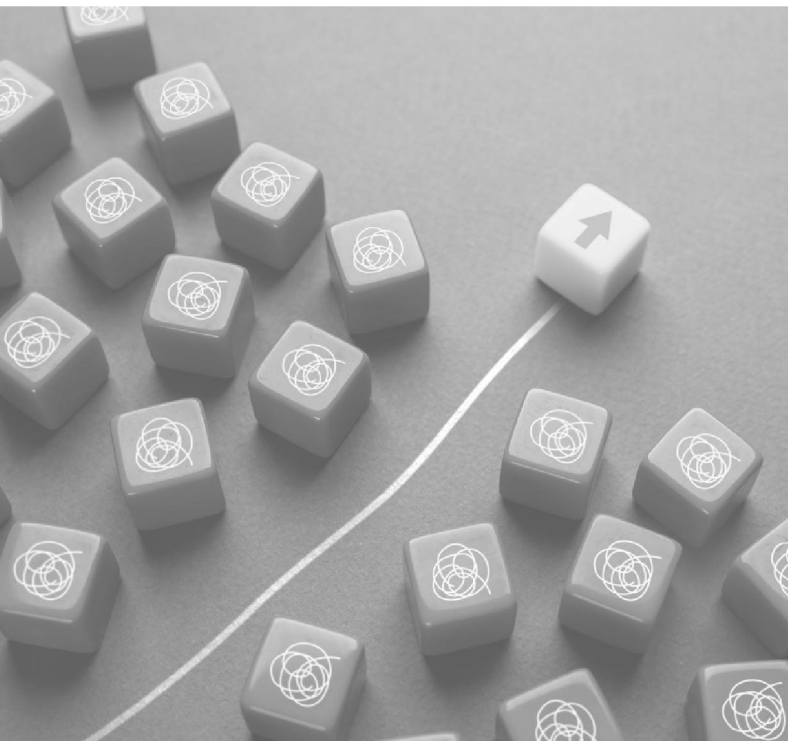
So verankern Sie kurzfristige Stabilität und langfristige Anpassungsfähigkeit in einer dynamischen Gesamtstrategie

controllit
Business Continuity Management

Inhalt

Einleitung

Organisational Resilience Management (ORM) ist ein wesentlicher Bestandteil einer zukunftssicheren Unternehmensstrategie. Es ermöglicht Organisationen, sich nicht nur auf regulatorische Anforderungen wie Digital-Operational-Resilience-Act-Verordnung (DORA), die Network and Information Security Directive 2 (NIS2) oder die Critical Entities Resilience Directive (KRITIS-Dachgesetz) vorzubereiten, sondern auch, unvorhergesehene Herausforderungen effektiv zu bewältigen.



Während die genannten Regelwerke vorrangig die Operational Resilience in den Fokus nehmen, um die Widerstandsfähigkeit kritischer Funktionen (technischer Systeme und Prozesse) sicherzustellen, geht der entscheidende Schritt darüber hinaus: die Entwicklung einer Organisational Resilience. Diese zielt darauf ab, die gesamte Organisation – von der Kultur über die Strategie bis hin zur Governance – auf langfristige Widerstandsfähigkeit auszurichten.

In vielen Unternehmen sind Konzepte für Operational Resilience vorhanden, auch wenn diese oft nicht explizit als solche benannt werden. Häufig fehlt jedoch die notwendige systemische Verzahnung der einzelnen Managementsysteme, um tatsächlich als Operational Resilience zu gelten. Die Ausweitung auf die organisatorische Ebene stellt jedoch eine größere Kraftanstrengung dar und erfordert eine systematische Vorgehensweise.

Dieses Whitepaper präsentiert die Herausforderungen und verdeutlicht die Unterschiede zwischen Operational und Organisational Resilience. Zudem wird ein ganzheitlicher Ansatz zur Implementierung eines ORM vorgestellt. Ziel ist es, kurzfristige Stabilität und langfristige Anpassungsfähigkeit durch eine abgestimmte Gesamtstrategie zu verbinden und als zentrale Aufgabe zu bearbeiten.

Kontext und Ausgangslage

Die aktuellen Anforderungen, Risiken und Herausforderungen sind komplex und dynamisch. Im Folgenden werden die zentralen Herausforderungen skizziert, denen Unternehmen gegenüberstehen:

- **Regulatorische Anforderungen** wie der Digital Operational Resilience Act (DORA), die Network and Information Security Directive 2 (NIS2) und das KRITIS-Dachgesetz verlangen umfassende Maßnahmen. Diese Regelwerke setzen klare Rahmenbedingungen, die Unternehmen dazu verpflichten, ihre Prozesse anzupassen, um Resilienz zu gewährleisten.
- Zu den **technologischen Risiken** zählen Cyberangriffe, die sensible Daten und Geschäftsprozesse gefährden. Ebenso kritisch sind Systemausfälle, die den operativen Betrieb unterbrechen können, sowie datenbasierte Störungen wie Manipulation oder Verlust wichtiger Informationen.
- **Marktdynamiken, Wirtschaftskrisen, technologische Disruptionen, Talentmangel und strategische Fehlentscheidungen** können Unternehmen in kritische Situationen bringen. Diese Herausforderungen führen zu erhöhtem Wettbewerbsdruck und beeinträchtigen die Fähigkeit von Organisationen, sich effektiv an neue Rahmenbedingungen anzupassen.
- **Gesellschaftliche und ökologische Herausforderungen wie Lieferkettenunterbrechungen, Ressourcenknappheit oder Umweltkatastrophen** stellen die Reaktionsfähigkeit von Unternehmen auf die Probe und erfordern eine zunehmende Anpassung an dynamische Umweltbedingungen und soziale Anforderungen.

Um diesen Anforderungen, Risiken und Herausforderungen gerecht zu werden, bedarf es einer strategischen Kombination aus Operational und Organisational Resilience. Operational Resilience stabilisiert kritische Funktionen, während Organisational Resilience die langfristige Anpassungsfähigkeit sicherstellt. Die Kombination beider Ansätze befähigt Unternehmen, flexibel und robust auf verschiedene Herausforderungen zu reagieren.

Differenzierung: Operational vs. Organisational Resilience

Operational und Organisational Resilience sind zwei unterschiedliche, aber komplementäre Ansätze, mit denen Unternehmen ihre Widerstandsfähigkeit stärken können.

Eine Gegenüberstellung:

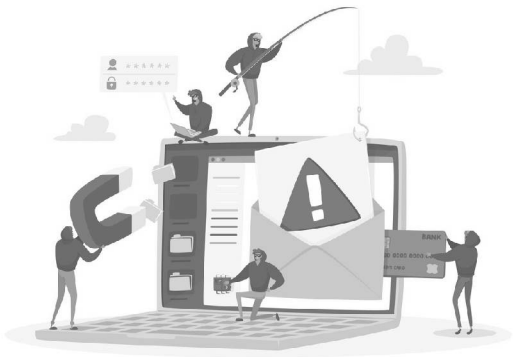
Kriterium	Operational Resilience	Organisational Resilience
Zeithorizont	Kurzfristig: Stabilität und Aufrechterhaltung kritischer Funktionen in akuten Störungen	Langfristig: Anpassungsfähigkeit und strategische Neuausrichtung über einen erweiterten Zeitraum
Ziele	Minimierung von Störungen, Wiederanlauf, Wiederherstellung und Stabilisierung der kritischen Funktionen	Aufbau langfristiger Widerstandsfähigkeit, Verbesserung der Wettbewerbsfähigkeit und Innovationskraft
Fokus	Prozesse, Systeme, technische Infrastruktur, physische Sicherheit, personelle Sicherheit	Unternehmenskultur, Governance, strategische Führung, Kommunikation
Relevante Bereiche	Business Continuity, Krisenmanagement, Informationssicherheit, physische Sicherheit, Security Management, Risikomanagement etc.	Strategisches Management, Organisationsentwicklung, Innovationsförderung, Führung, Stakeholder-Management etc.
Typische Bedrohungen	Cyberangriffe, Naturkatastrophen, technische Ausfälle, Lieferkettenunterbrechungen, Betriebsunterbrechungen etc.	Regulatorische Veränderungen, Marktveränderungen, gesellschaftliche Trends etc.
Risiken	Fehlende Verfügbarkeit von IT-Systemen, Personalmangel, physische Schäden an Infrastrukturen etc.	Strategische Fehlausrichtung, fehlende Anpassungsfähigkeit, Kommunikationsdefizite in Krisenzeiten etc.
Methoden und Modelle	Business-Impact-Analyse, Schutzbedarfsfeststellung, Gap-Analyse, Bedrohungsanalyse, Fehlermöglichkeits- und Einfluss-Analyse etc.	SWOT-Analyse, PESTEL-Analyse, Stakeholder-Identification-Analyse, Szenarioplanung etc.

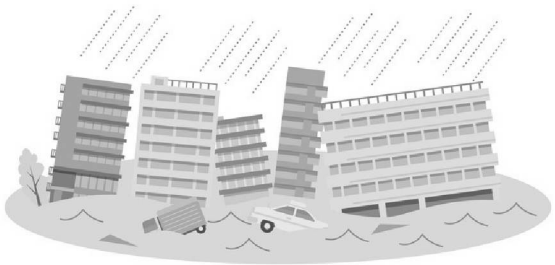
Differenzierung: Operational vs. Organisational Resilience

Operational und Organisational Resilience an Beispielen erläutert:

Lieferkettenunterbrechung:
Operational Resilience stellt bei Lieferkettenunterbrechungen sicher, dass alternative Lieferwege etabliert sind, während Organisational Resilience es ermöglicht, strategische Partnerschaften und flexible Prozesse zu entwickeln, um auf langfristige Marktveränderungen zu reagieren.

Cyberangriff:
Operational Resilience sorgt bei Cyberangriffen für technische Sicherheitsmaßnahmen wie Firewalls und Echtzeitüberwachung, während Organisational Resilience Schulungen und Kommunikationsstrategien umfasst, um langfristige Risiken zu minimieren.



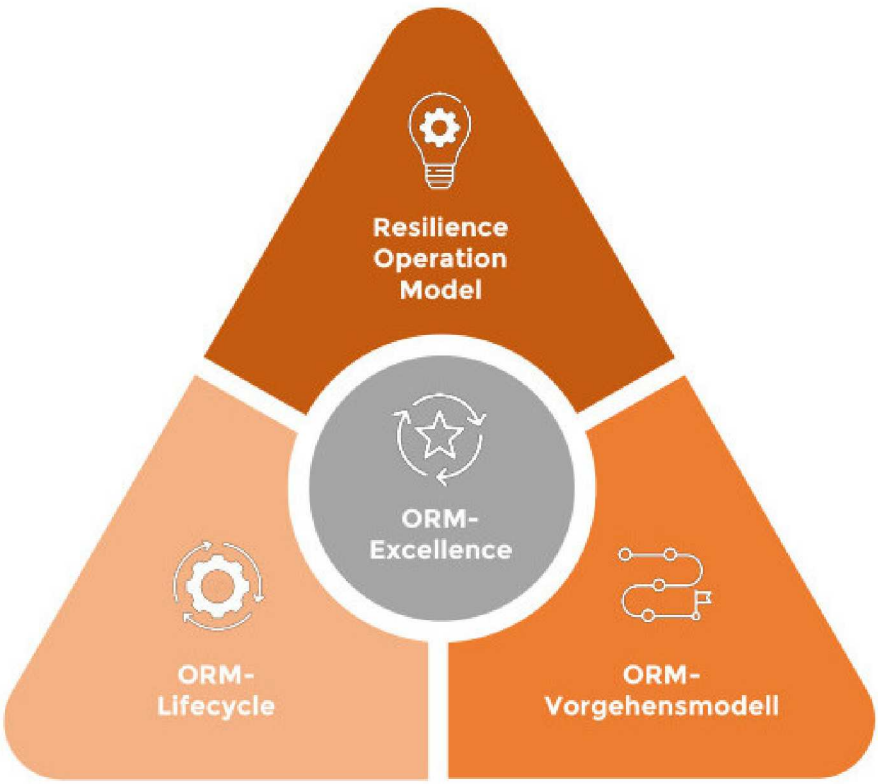


Naturkatastrophen:
Operational Resilience beinhaltet bei Naturkatastrophen Schutzmaßnahmen wie Evakuierungspläne und redundante Standorte. Organisational Resilience fokussiert auf langfristige Notfallpläne und Partnerschaften zur Ressourcenbereitstellung.

Produktionsausfall:
Operational Resilience sorgt bei Produktionsausfällen dafür, dass redundante Fertigungsstandorte aktiviert werden können, während Organisational Resilience durch strategische Planung und Investitionen in alternative Märkte eine langfristige Anpassung ermöglicht.

Die Umsetzung von Organisational Resilience Management

Für die Umsetzung eines ORM empfiehlt sich eine Verzahnung aus dem Resilience Operation Model (ROM), dem ORM-Vorgehensmodell und dem ORM-Lifecycle.



Das ROM stellt die strategische Vision und Ausrichtung dar und bleibt während aller Phasen als grundlegendes Rahmenwerk bestehen. Das ORM-Vorgehensmodell wiederum wird als pragmatischer Leitfaden für die Erstimplementierung genutzt, um die Strategien und Ziele des ROM in operative Realität umzusetzen. Der ORM-Lifecycle beginnt nach der Erstimplementierung für den Regelbetrieb und umfasst einen kontinuierlichen Prozess der Überprüfung, Anpassung und Verbesserung, wobei die Prinzipien des ROM als Leitfaden dienen.

Die Umsetzung von Organisational Resilience Management

Synergien anhand von zwei Beispielen dargestellt:

	Strategie in Aktion	Fortlaufende Verbesserung	Strategieanpassung
Cyberangriffe	Ein Unternehmen definiert im ROM, dass die Stärkung der IT-Sicherheit ein zentrales Ziel ist. Das ORM-Vorgehensmodell konkretisiert dies durch die Einführung eines Incident-Management-Systems und die Schulung von Mitarbeitenden.	Die Maßnahmen aus dem ORM-Vorgehensmodell werden im Lifecycle regelmäßig überprüft und weiterentwickelt, um neue Sicherheitsstandards und/oder technologische Entwicklungen zu integrieren.	Erkenntnisse aus dem Lifecycle, zum Beispiel über die Effektivität bestimmter Maßnahmen, fließen in die Weiterentwicklung der strategischen Ausrichtung des ROM ein.
Technische Disruption	Das ROM bietet die strategische Grundlage, um auf technologische Disruptionen wie neue Geschäftsmodelle oder Wettbewerber zu reagieren. Disruptive Technologien erfordern Investitionen in Forschung und die Identifikation neuer Geschäftsfelder.	Das Vorgehensmodell überführt strategische Vorgaben in Maßnahmen zur operativen Vorbereitung auf technologische Disruptionen. Dazu gehören agile Methoden, ein Innovationsmanagement und Prozesse zur schnellen Integration neuer Technologien.	Der Lifecycle sorgt für Flexibilität und kontinuierliche Anpassung an technologische Veränderungen. Innovationsworkshops und Marktfeedback helfen, neue Trends frühzeitig zu erkennen und zu nutzen.

Ausgangslage analysieren und Weichen stellen

Die Analyse der Ausgangslage hilft dabei, organisationale Schwächen, externe Bedrohungen sowie strategische Potenziale systematisch zu identifizieren. Diese Erkenntnisse bilden die Grundlage für zielgerichtete Maßnahmen im ORM.

Ist-Analyse

Die Ist-Analyse basiert auf dem ROM-Zielmodell und wird mit ergänzenden Methoden durchgeführt. Das Ziel besteht darin, Stärken, Schwächen und Handlungsfelder strukturiert sichtbar zu machen, die anschließend in den Entwicklungsplan einfließen.

Schritte	Erläuterungen
Rahmen und Zielsetzung definieren	Definition der Zielsetzung, Analysebereiche und Stakeholder zur strategischen Ausrichtung der Analyse
Datensammlung	Durchführung von Interviews, Workshops und technischer Dokumentenanalyse
Analyse und Bewertung	Anwendung des ROM-Zielmodells zur qualitativen Reifegradbestimmung, ergänzend: SWOT/PESTEL zur Umfeldbetrachtung
Ableitung des Resilienz-strategiekonzepts	Überführung in strategische Zielkategorien (Schutz, Erhalt und Risikominderung) und Handlungsfelder
Entwicklung eines Umsetzungsplans	Priorisierung der Handlungsfelder, Formulierung erster strategischer und operativer Maßnahmen sowie Freigabe der Investitionen

ROM-Zielmodell: Reifegradanalyse für Operational und Organisational Resilience

Im Rahmen eines ORM ist das ROM-Zielmodell ein zentraler strategischer Ansatz. Dieses Modell verbindet systematisch die strategischen Vorgaben des ROM mit klar definierten Resilienzzielen und der operativen Umsetzung.

Kernpunkte des ROM-Zielmodells
Das ROM-Zielmodell bildet die Basis für die Ableitung und Steuerung von Resilienzzielen und deren kontinuierliche Verbesserung. Dabei werden insbesondere folgende Aspekte berücksichtigt:

- Verbindung ROM und Zielmodell: Das ROM bietet den strategischen Rahmen, aus dem konkrete Resilienzziele abgeleitet und im Zielmodell operationalisiert werden.
- Reifegradbewertung: kontinuierliches Monitoring des Erreichungsgrads der definierten Ziele über geeignete Kennzahlen
- Strategische Zielableitung: Ableitung messbarer Resilienzziele, die systematisch in das Resilienz-Controlling überführt werden
- Steuerung und Optimierung: regelmäßige Überprüfung und Anpassung der Ziele und Maßnahmen zur nachhaltigen Steigerung der Resilienz

Vom ROM-Zielmodell zum Resilienzstrategiekonzept
Das ROM-Zielmodell schafft die Grundlage für die Entwicklung des Resilienzstrategie-konzepts. Dieses Konzept konkretisiert die strategischen Ziele in umsetzbare Maßnahmen und definiert Prozesse zur operativen Realisierung. Durch klare, messbare Vorgaben wird sichergestellt, dass strategische Zielsetzungen effektiv umgesetzt und kontinuierlich verbessert werden.

Umsetzungsplanung als nächster Schritt
Die Umsetzungsplanung konkretisiert die Maßnahmen des Resilienzstrategiekonzepts und ordnet diesen klare Verantwortlichkeiten und Prioritäten zu. Die Integration in das Resilienz-Controlling ermöglicht eine transparente Steuerung, regelmäßige Erfolgs-messung und kontinuierliche Optimierung auf Basis belastbarer Daten und Erkenntnisse.

Fazit

Die wirksame Umsetzung eines ORM basiert auf der Fähigkeit, strategische Ziele, operative Maßnahmen und kontinuierliche Anpassung systemisch zu verzahnen. Das ROM-Zielmodell hilft bei der strategischen Umsetzung.

Key Takeaways:

- Unternehmen müssen regulatorische Anforderungen und dynamische Risiken gleichermaßen adressieren. Entscheidend ist eine integrierte, vorausschauende Resilienzstrategie.
- Operational und Organisational Resilience ergänzen sich. Während die eine kurzfristige Stabilität sichert, schafft die andere langfristige Anpassungsfähigkeit.
- Ein durchdachtes Konzept, das vom strategischen Ziel über die Umsetzung bis zur kontinuierlichen Verbesserung reicht, ist essenziell für eine zukunftsfähige Organisation.
- Eine strukturierte Ist-Analyse sowie ein darauf aufbauender Umsetzungsplan ermöglichen eine schrittweise, nachvollziehbare Resilienzsteigerung.
- Das ROM-Zielmodell bildet die Grundlage für eine systematische Zielableitung, Reifegradbewertung und die Steuerung durch Objectives and Key Results sowie Key Performance Indicators im Resilienz-Controlling.

Die Verbindung von Strategie, Umsetzung und kontinuierlicher Verbesserung ist essenziell, um Unternehmen widerstandsfähiger zu machen und ihnen einen nachhaltigen Wettbewerbsvorteil zu verschaffen. Resilienz ist kein statischer Zustand, sondern ein fortwährender Prozess, der in die DNA jeder Organisation integriert sein sollte.

Sie haben Fragen zum Thema? Melden Sie sich gern bei uns!

Controllit AG
Kühnehöfe 20
22761 Hamburg
Deutschland
www.controll-it.de

Stand: Juli 2025

Die Controllit AG ist Ihr Partner für Business Continuity Management (BCM). Seit unserer Gründung entwickeln wir integrative Konzepte und Produkte für das Business Continuity Management, IT Service Continuity Management, Information Security Management und Krisenmanagement. Wir helfen Ihnen mit strategischen, organisatorischen und technischen Konzepten, Ihre Geschäftsprozesse gegen Bedrohungen abzusichern und für Notfälle vorzusorgen.

Foto-/Grafiknachweise: Titel: iStock.com/Yossakorn Kaewwannarat; S. 3: iStock.com/bagira22; S. 6: iStock.com/Veysel Celikdemir, iStock.com/lemono, iStock.com/morita kenjiro, iStock.com/SiberianArt; S. 8: iStock.com/z_wei; S. 9: iStock.com/VectorMine; S. 12: iStock.com/metamorworks