



Whitepaper

Intelligente Resilienz

Der Wandel von reaktiver
Planung zu
vorausschauender
Anpassung



controllit
Business Continuity Management ■



Inhalt

03

Einleitung

04

Das Gebot der Resilienz: jenseits statischer Planung

06

Das neue Paradigma: integriertes Organisational Resilience Management

08

KI als Katalysator für intelligente Resilienz

10

Der KI-gestützte Resilienz-Lebenszyklus in der Praxis

12

Die Zukunft der Vorbereitung: Simulation mit digitalen Zwillingen

13

Von der Analyse zur Antizipation: die lernende Organisation schaffen

14

Strategischer Fahrplan zur Implementierung

15

Fazit und strategische Empfehlungen



Einleitung

Die Fähigkeit, auf unvorhersehbare Störungen und stetigen Wandel zu reagieren, ist für den nachhaltigen Erfolg von Unternehmen essenziell. Traditionelle, isoliert betrachtete Resilienzdisziplinen wie das Business Continuity Management (BCM) sind der heutigen dynamischen und komplexen Risikolandschaft jedoch nicht mehr gewachsen und setzen Unternehmen erheblichen finanziellen, rechtlichen und reputativen Risiken aus. Unser Whitepaper skizziert den nächsten logischen Entwicklungsschritt: den Wandel von der dokumentenbasierten Business Continuity hin zu einem durch künstliche Intelligenz gestützten, proaktiven und ganzheitlichen Organisational Resilience Management (ORM).



Der wesentliche Katalysator für diese Transformation ist die künstliche Intelligenz (KI). KI ermöglicht es Organisationen, den gesamten Resilienz-Lebenszyklus neu zu gestalten: von der vorausschauenden Risikoerkennung durch Echtzeit-Analyse globaler Datenströme über die dynamische, automatisierte Business-Impact-Analyse bis hin zur intelligenten Entscheidungsunterstützung und automatisierten Reaktion im Krisenfall. Technologien wie Predictive Analytics, Machine Learning und digitale Zwillinge transformieren die Vorbereitung von einer periodischen Übung in eine kontinuierliche, messbare Simulation der Widerstandsfähigkeit.

Die Implementierung ist jedoch keine rein technische Initiative. Sie erfordert eine strategische Verpflichtung zu exzellenter Datenqualität und -Governance, die Etablierung eines Human-in-the-Loop-Ansatzes, der menschliche Expertise mit maschineller Effizienz verbindet, und die Auseinandersetzung mit kritischen ethischen Fragen. Dieses Whitepaper liefert Führungskräften und Fachexperten einen strategischen Fahrplan, um eine intelligente Resilienzfähigkeit aufzubauen, die nicht nur Risiken minimiert, sondern einen nachhaltigen Wettbewerbsvorteil in einer unsicheren Zukunft sichert. Der Übergang von reaktivem Wiederanlauf und reaktiver Wiederherstellung zu proaktiver, vorausschauender Anpassungsfähigkeit ist nicht länger eine Option, sondern eine strategische Notwendigkeit.



Das Gebot der Resilienz: jenseits statischer Planung

Die moderne Geschäftswelt operiert in einem Umfeld, das durch Volatilität, Unsicherheit, Komplexität und Ambiguität (VUCA) sowie durch Brüchigkeit, Angst, Nichtlinearität und Unverständlichkeit (BANI) gekennzeichnet ist. Diese Rahmenwerke beschreiben eine Realität, in der traditionelle Methoden des Risikomanagements und der Notfallplanung, die auf statischen, linearen Annahmen beruhen, unzureichend sind.

Das klassische BCM bildet das notwendige und bewährte Fundament für die Stabilität von Organisationen. Angesichts der zunehmenden Vernetzung und Dynamik globaler Risiken wird jedoch deutlich, dass dieser wichtige Schutz um eine strategische und vorausschauende Perspektive ergänzt werden muss. Die Diskussion um die Zukunft der Resilienz konzentriert sich daher auf die Weiterentwicklung bestehender Ansätze in folgenden Bereichen:

- Die Konzentration auf bekannte, isolierte Risiken führt zu einer **unzureichenden Risikobewertung**, die oft die komplexe Natur systemischer Bedrohungen ignoriert und auf unrealistischen Annahmen beruht.
- In dynamischen Organisationen führt die ständige Veränderung von Prozessen und Personal zu einer **mangelnden Aktualisierung der Pläne**, die im Krisenfall oft bereits veraltet sind.
- Durch **fehlende Tests und realistische Übungen** bleiben kritische Schwachstellen, Abhängigkeiten und Fehlannahmen in den Plänen unentdeckt.
- Durch **mangelnde Individualisierung** können Standardvorlagen die spezifischen Risiken und Anforderungen, die sich aus Branche, Standort und Unternehmensgröße ergeben, nicht immer adäquat abbilden.
- Eine **starre Erwartungshaltung** in Plänen geht oft von einem linearen, vorhersehbaren Ablauf aus und vernachlässigt unvorhergesehene Abweichungen.

Diese prozessualen Schwächen werden durch organisatorische Hürden wie fehlende Ressourcen und mangelnde Unterstützung durch das Management verschärft. Die Konsequenzen sind gravierend: finanzielle Verluste, Reputationsschäden, rechtliche Konsequenzen und interne Betriebsstörungen.



Das Gebot der Resilienz: jenseits statischer Planung

Das Kernproblem ist somit nicht, dass Pläne schlecht aktualisiert werden, sondern dass das gesamte Paradigma der statischen Planung versagt hat. Unternehmen, die weiterhin nur in die Verfeinerung traditioneller BCM-Prozesse investieren, ohne das zugrunde liegende Paradigma zu ändern, investieren in eine trügerische Sicherheit. Sie führen die sichtbaren Aktivitäten der Resilienz durch – das Schreiben von Plänen, das Abhalten von Meetings –, ohne die tatsächliche Fähigkeit zur Anpassung zu erlangen. Dies stellt eine strategische Fehlallokation von Ressourcen dar. Die Herausforderung besteht also nicht darin, Pläne besser zu machen, sondern darin, einen grundlegend anderen, dynamischen Ansatz für Resilienz zu entwickeln.





Das neue Paradigma: integriertes Organisational Resilience Management

Als Antwort auf die Unzulänglichkeiten statischer Planung hat sich das ORM als neues, übergeordnetes Paradigma herauskristallisiert. Es markiert einen strategischen Wandel von reaktivem Wiederanlauf und reaktiver Wiederherstellung hin zur proaktiven Stärkung der Widerstands- und Anpassungsfähigkeit der gesamten Organisation. Die folgende Tabelle grenzt die zentralen Begriffe voneinander ab.

Überblick über die Resilienzkonzepte

Fähigkeit	Fokus	Zeithorizont
Krisenmanagement	Strategische Reaktion auf ein kritisches Ereignis zum Schutz von Leben, Werten und Reputation durch effektive Entscheidungsfindung und Kommunikation	kurz- bis mittelfristig
Business Continuity	Sicherstellung der Verfügbarkeit von zeitkritischen Geschäftsprozessen im Ereignisfall auf einem vordefinierten, akzeptablen Niveau	kurz- bis mittelfristig
IT Service Continuity	Sicherstellung der Verfügbarkeit der IT-Infrastruktur und -Services zur Unterstützung zeitkritischer Geschäftsprozesse	kurz- bis mittelfristig
Operational Resilience	Minimierung von Störungen, Wiederanlauf, Wiederherstellung und Stabilisierung der kritischen Funktionen	kurz- bis mittelfristig
Organisational Resilience	Aufbau langfristiger Widerstandsfähigkeit, Verbesserung der Wettbewerbsfähigkeit und Innovationskraft	mittel- bis langfristig



Das neue Paradigma: integriertes Organisational Resilience Management

ORM bildet einen ganzheitlichen Rahmen, der traditionelle Disziplinen wie Operational Risk Management, BCM, Krisenmanagement (KM), IT Service Continuity Management (ITSCM), Informationssicherheitsmanagement (ISM) und Third-Party Risk Management integriert. Ziel ist es, organisatorische Silos aufzubrechen und Widerstandsfähigkeit in allen wesentlichen Bereichen und Prozessen des Unternehmens zu verankern.

Operational Resilience nimmt hierbei eine besondere Rolle ein: Sie bündelt die operativen Disziplinen und koordiniert ihre Zusammenarbeit, um die Widerstandsfähigkeit kritischer Geschäftsprozesse und Dienstleistungen im laufenden Betrieb sicherzustellen. Damit schafft sie die Grundlage, auf der die strategische, kulturelle und ganzheitliche Widerstandsfähigkeit des ORM aufbaut.

Organisational Resilience Management (ORM) ersetzt etablierte Disziplinen wie BCM nicht, sondern erweitert sie. Ein wirksames BCM liefert weiterhin die notwendigen Strategien für Wiederanlauf und Wiederherstellung in der Krise und beim kritischen Vorfall und bleibt damit ein unverzichtbarer Baustein umfassender Resilienz. Der entscheidende Übergang liegt jedoch darin, dass ORM mehr ist als prozessuale Integration: Es steht für einen fundamentalen kulturellen Wandel. Resilienz entwickelt sich von einer isolierten, compliance-getriebenen Aufgabe zu einer unternehmensweiten strategischen Fähigkeit. Sie wird zu einer Kennzahl auf dem Executive-Dashboard, zu einem festen Bestandteil der Unternehmenskultur und zu einer aktiven Managementaufgabe des C-Levels und des Vorstands. Dadurch verändert sich, wie Resilienz finanziert, gemessen und verantwortet wird – nicht mehr als Kostenfaktor, sondern als strategische Investition in die Zukunftsfähigkeit des Unternehmens.





KI als Katalysator für intelligente Resilienz

Der strategische Wandel hin zur Organisational Resilience wird durch künstliche Intelligenz (KI) ermöglicht und beschleunigt. KI ist kein inkrementelles Upgrade, sondern ein fundamentaler Game-Changer, der den Paradigmenwechsel von reaktiven hin zu proaktiven und vorausschauenden Strategien erzwingt. Ihre Fähigkeit, riesige Datenmengen in Echtzeit zu analysieren, erlaubt es, subtile Muster und aufkommende Bedrohungen zu erkennen, lange bevor sie zur Krise werden. Zu den Schlüsseltechnologien gehören:

- Mithilfe von **Predictive Analytics** werden historische Daten und Machine Learning genutzt, um zukünftige Ereignisse vorherzusagen und Störungen zu antizipieren.
- Beim **Machine Learning** (ML) lernen Algorithmen selbstständig aus Daten, um Muster zu erkennen, Vorhersagen zu treffen und Prozesse zu automatisieren.
- Das **Natural Language Processing** (NLP) verleiht Maschinen die Fähigkeit, unstrukturierte Datenquellen wie Nachrichten oder Social-Media-Beiträge zu verstehen, die oft erste Krisensignale enthalten.

Der Erfolg jeder KI-Initiative steht und fällt jedoch mit der Qualität der Daten. Die bloße Menge an Daten führt nicht automatisch zu besseren Ergebnissen ("mehr Daten" ist nicht gleich "bessere KI"). Die Grundlage für intelligente Resilienz sind AI-Ready Data, die auf drei zentralen Grundlagen ruhen: Datenqualität, kontextuelle Relevanz für den Anwendungsfall und eine robuste Daten-Governance zur Gewährleistung von Sicherheit, Datenschutz und Compliance.



KI als Katalysator für intelligente Resilienz

Die strengen Anforderungen der KI wirken als starker Impulsgeber, der Organisationen dazu zwingt, seit langem bestehende Probleme anzugehen. Organisationen müssen insbesondere folgende Herausforderungen angehen:

- Es müssen **Datensilos aufgebrochen** werden, damit Informationen aus verschiedenen Abteilungen und Systemen zusammengeführt und zugänglich gemacht werden.
- Die **Verbesserung der Datenqualität** ist essenziell, indem mangelhafte, inkonsistente oder veraltete Daten bereinigt und standardisiert werden.
- Es bedarf der **Etablierung einer zentralen Governance**, um fragmentierte Zuständigkeiten für Daten in einem klaren Regelwerk für Datenmanagement und -sicherheit zu bündeln.

Der eigentliche strategische Mehrwert liegt in dem hochwertigen, zentralisierten Daten-Asset, das durch diesen Prozess geschaffen wird. Dieser neu geschaffene, aus internen wie externen Quellen zusammengeführte und qualitativ aufbereitete Datenpool verändert die Berechnung des Return on Investment (ROI) fundamental. Der Business Case beschränkt sich nicht mehr nur auf die Vermeidung von Ausfallkosten, sondern umfasst den Wert, den diese neue, unternehmensweite Datenfähigkeit für andere Geschäftsbereiche – vom Marketing bis zur Finanzplanung – schafft und so die digitale Transformation im gesamten Unternehmen beschleunigt. Die Investition wird so von einem Kostenfaktor zu einem strategischen Wegbereiter.





Der KI-gestützte Resilienz-Lebenszyklus in der Praxis

KI revolutioniert jede Phase des Resilienz-Lebenszyklus und ermöglicht den Übergang von periodischen, manuellen Tätigkeiten zu kontinuierlichen, datengesteuerten Abläufen.

Proaktive Bedrohungsanalyse & vorausschauende Risikoerkennung

Traditionelle Risikobewertungen sind statisch und blicken zurück. KI-gestützte Risiko-Intelligenz-Plattformen überwinden diese Einschränkung durch die kontinuierliche Echtzeitanalyse heterogener Datenquellen wie IoT-Sensordaten, Social Media, Nachrichten und Logistikdaten. In der Praxis bedeutet das beispielsweise:

- Bei einer drohenden **Lieferkettenstörung** können KI-Modelle Engpässe vorhersagen, indem sie Wetterdaten mit Schiffsrouten korrelieren oder die finanzielle Stabilität kritischer Lieferanten überwachen.
- Um **Cyber-Bedrohungen** zu erkennen, identifizieren ML-Algorithmen subtile Anomalien im Netzwerkverkehr, anstatt nur auf bekannte Signaturen zu reagieren, und können so auch Angriffe aufdecken, die für traditionelle Antivirenprogramme unsichtbar sind.
- Durch die Analyse von Nachrichten können Unternehmen frühzeitig vor **geopolitischen Risiken** gewarnt werden, beispielsweise vor Unruhen in Regionen mit kritischen Zulieferern.

Dynamische Business-Impact-Analyse (BIA) & Abhängigkeits-Mapping

Die traditionelle BIA ist ein zeitaufwendiger, oftmals manueller Prozess, dessen Ergebnisse schnell veralten. KI transformiert die BIA von einer statischen Momentaufnahme zu einem dynamischen, kontinuierlichen Monitoring.

- Eine KI erstellt eine **lebende Landkarte** der Organisation, indem sie direkt auf operative Systeme zugreift und automatisch eine dynamische Abhängigkeitskarte der Prozesse und IT-Systeme generiert.
- Fällt ein Server aus, berechnet das System unmittelbar den genauen **Blast Radius**, also welche Geschäftsprozesse betroffen sind, wie hoch der finanzielle Schaden ist und welche Kunden betroffen sind, wodurch verborgene Schwachstellen aufgedeckt werden.



Der KI-gestützte Resilienz-Lebenszyklus in der Praxis

Intelligente Lageerfassung & Entscheidungsunterstützung

Im Krisenfall ist ein einheitliches Lageverständnis unerlässlich. KI entwickelt das traditionelle Common Operating Picture – also ein gemeinsames, einheitliches Lagebild – von einer reinen Visualisierungsplattform zu einem intelligenten Entscheidungssystem weiter.

- Mithilfe von Bilderkennung auf Drohnenaufnahmen kann eine KI die **Schadensbewertung** nach einem Sturm massiv beschleunigen und das Ausmaß der Zerstörung von Anlagen in Minuten statt Tagen bewerten.
- Basierend auf Wetter- und Logistikdaten kann die KI eine **Krisenprognose** erstellen, beispielsweise über die Auswirkungen eines Hurrikans auf geplante Lieferungen.
- Dank **Explainable AI** agiert die KI als Crisis Strategy Coach, der nachvollziehbare Begründungen für seine Empfehlungen liefert und so das Vertrauen menschlicher Entscheider gewinnt.

Automatisierte Reaktion & Wiederherstellung

KI ermöglicht die Automatisierung zeitkritischer Reaktionsprozesse, was die Reaktionszeit drastisch verkürzt und das Risiko menschlicher Fehler unter Druck minimiert.

- Spezialisierte Krisenmanagement-Plattformen lösen bei einem definierten Ereignis eine **automatisierte Kommunikation** aus und aktivieren Alarmierungs- und Kommunikationskaskaden.
- Erkennt die KI einen Lieferantenausfall, kann sie sofort Alternativen analysieren und ein **dynamisches Rerouting** von Warenströmen initiieren.
- Basierend auf dem dynamischen Lagebild kann eine KI die **intelligente Ressourcenallokation** steuern und bei einem Cyberangriff IT-Ressourcen umschalten oder bei einem Produktionsausfall Wartungsteams anleiten.

Die wahre Revolution liegt in der nahtlosen Integration dieser Anwendungen zu einem semiautomen Resilienzsystem. Dies verändert die Rolle des Krisenmanagers maßgeblich: Er wird vom reaktiven Ersthelfer zum strategischen Mission Controller, der ein intelligentes System überwacht und sich auf übergeordnete strategische und ethische Entscheidungen konzentriert.



Die Zukunft der Vorbereitung: Simulation mit digitalen Zwillingen

Traditionelle Übungen und Tests sind oft qualitativ und auf wenige Szenarien beschränkt, da sie ressourcenintensiv sind und meist nur eine begrenzte Anzahl an Störungen realistisch abbilden können. Um Resilienz wirklich zu testen, bedarf es einer revolutionären Technologie: des digitalen Zwillings. Ein digitaler Zwilling ist eine exakte virtuelle Nachbildung eines Prozesses oder Systems, die kontinuierlich mit Echtzeitdaten gespeist wird und so den Zustand ihres Gegenstücks dynamisch widerspiegelt.

Diese Technologie schafft eine risikofreie Sandbox-Umgebung, in der Organisationen ihre Notfallpläne unter hyperrealistischen Bedingungen testen können, ohne den laufenden Betrieb zu gefährden. Anstatt qualitativer Diskussionen liefert die Simulation quantitative Metriken (z. B. genaue Wiederanlaufzeiten oder Datenverlusten) zur Überprüfung der Wirksamkeit von Plänen. Konkrete Anwendungsfälle sind unter anderem:

- Unternehmen können **Supply-Chain-Stresstests** durchführen, um den Ausfall eines Lieferanten oder die Blockade eines Hafens zu simulieren und Engpässe präzise aufzuzeigen.
- Sicherheitsteams können **simulierte Cyberangriffe** auf den digitalen Zwilling ihrer IT-Infrastruktur starten, um die Wirksamkeit von Sicherheitskontrollen und IT Recovery Plänen in einer sicheren Umgebung zu validieren.
- Ein erheblicher Vorteil ist die **Validierung von Wiederanlaufparametern**, da eine Simulation aufdecken kann, ob z. B. ein definiertes Recovery Time Objective (RTO) unter realeren Bedingungen eingehalten werden kann.

Der Einsatz von digitalen Zwillingen überführt die Resilienzplanung von einer auf qualitativen Annahmen basierenden Disziplin in eine empirisch fundierte Disziplin. Dies hebt die Anforderungen an die unternehmerische Sorgfaltspflicht auf eine neue Ebene. Wenn ein Werkzeug zur empirischen Überprüfung von Plänen existiert, könnte es bei einer rechtlichen oder regulatorischen Prüfung nach einem Vorfall als Managementversäumnis gewertet werden, sich weiterhin nur auf ungetestete Annahmen verlassen zu haben.

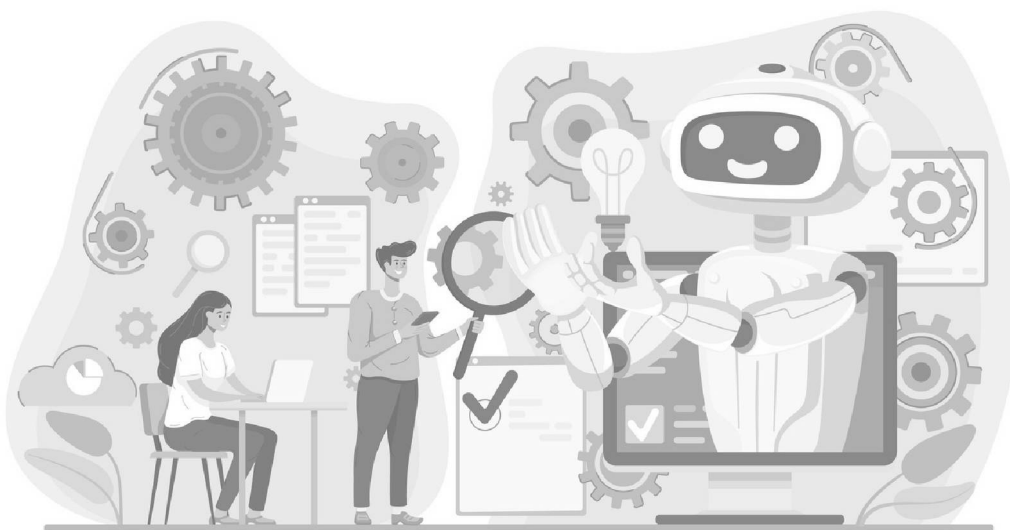


Von der Analyse zur Antizipation: die lernende Organisation schaffen

Der Resilienz-Lebenszyklus endet nicht mit der Bewältigung einer Krise. KI transformiert die Lessons-Learned-Phase, indem sie einen geschlossenen, sich selbst verbessernden Lernkreislauf schafft. Sie automatisiert die Ursachenforschung (Root Cause Analysis (RCA)) und macht sie schneller und objektiver. In der Praxis bedeutet das beispielsweise:

- Nach einem Vorfall kann eine KI durch eine **automatisierte RCA** in Minuten riesige Mengen an Log-Daten analysieren und Korrelationen aufdecken, die ein menschliches Team nur schwer finden würde.
- Eine **intelligente Planaktualisierung** geht über simple Datenabgleiche hinaus, indem ein KI-Agent beispielsweise interne Projektdokumentationen analysiert, um neu entstandene Abhängigkeiten proaktiv zu erkennen und Plan-Updates vorzuschlagen. Das geht über die einfache Aktualisierung von Kontaktdaten hinaus.

Die KI-Systeme lernen aus jedem Vorfall und jeder Übung. Die Risikomodelle werden verfeinert, die Simulationen realistischer und die Vorhersagegenauigkeit verbessert sich. Auf diese Weise schafft die KI eine Art persistentes, institutionelles Gedächtnis für Resilienz. Traditionelles Wissen geht oft durch Personalwechsel verloren; ein KI-gestütztes System hingegen verankert die Erkenntnisse in seiner eigenen Logik. Resilienz wird so von der Expertise Einzelner entkoppelt und zu einer intrinsischen, sich ständig verbessernden Eigenschaft des Managementsystems der Organisation. Es entsteht eine lernende Organisation, die eine Kaizen-ähnliche Philosophie der kontinuierlichen Verbesserung verkörpert.





Strategischer Fahrplan zur Implementierung

Die Einführung von KI-gestützter Resilienz ist eine strategische Initiative, die einen klaren Fahrplan und die Etablierung eines robusten Governance-Rahmens erfordert. Die größten Herausforderungen sind mangelnde Datenqualität (Garbage In, Garbage Out), die Rechtfertigung von Kosten und ROI, der Mangel an Fachkräften mit BCM- und KI-Expertise sowie die Integration in Altsysteme.

Der Human-in-the-Loop-Ansatz ist dabei von zentraler Bedeutung. KI ist ein Werkzeug zur Erweiterung menschlicher Fähigkeiten, kein Ersatz. Fachexperten validieren Ergebnisse, behandeln Ausnahmefälle und treffen die endgültigen strategischen Entscheidungen, während die KI datenintensive Aufgaben übernimmt.

Die folgende Tabelle fasst die zentralen Herausforderungen und die notwendigen strategischen Antworten zusammen.

Strategischer Fahrplan: Herausforderungen und Lösungsansätze

Herausforderung	Lösungsansatz und Governance-Maßnahme
Datenqualität	Aufbau einer unternehmensweiten Datenstrategie; Etablierung einer robusten Daten-Governance als Priorität
Kosten/ROI	Definition klarer Business Cases; Start mit gezielten Pilotprojekten mit hohem ROI, um den Wert nachzuweisen
Fachkräftemangel	Investition in die Weiterbildung von Mitarbeitern; Förderung einer Kultur der Zusammenarbeit zwischen Mensch und Maschine
Integration	Planung der nahtlosen Integration in bestehende Prozesse und Altsysteme zur Vermeidung von Datensilos
Ethische Risiken (Bias, XAI)	Proaktive Adressierung von algorithmischer Voreingenommenheit, Transparenz (Explainable AI) und Rechenschaftspflicht



Fazit und strategische Empfehlungen

Die Ära der statischen Business-Continuity-Pläne neigt sich dem Ende zu. Der Übergang zu einem proaktiven, intelligenten Organisational Resilience Management ist eine strategische Notwendigkeit. Selbst die beste Planung stößt bei extremen Black-Swan-Ereignissen an ihre Grenzen. In solchen Szenarien zeigt sich der wahre Wert von Organisational Resilience: eine anpassungsfähige Kultur, die in der Lage ist, auch ohne vordefiniertes Drehbuch zu improvisieren.

Für Führungskräfte und Fachexperten ergeben sich daraus folgende strategische Empfehlungen:

- **Etablieren Sie Organisational Resilience Management als strategisches Ziel.** Verankern Sie Resilienz in der Geschäftsstrategie, brechen Sie organisatorische Silos auf und fördern Sie eine Kultur der geteilten Verantwortung.
- **Investieren Sie in Datenreife als Priorität.** Erkennen Sie an, dass AI-Ready Data die Grundlage für intelligente Resilienz ist. Initiieren Sie eine unternehmensweite Datenstrategie zur Schaffung einer hochwertigen Datengrundlage.
- **Beginnen Sie mit gezielten Pilotprojekten.** Identifizieren Sie Anwendungsfälle mit hohem ROI, um den Wert von KI im Resilienz-Management zu demonstrieren und eine Grundlage für eine breitere Skalierung zu schaffen.
- **Fördern Sie eine Human-in-the-Loop-Kultur.** Stellen Sie sicher, dass KI als Werkzeug zur Unterstützung menschlicher Expertise verstanden wird, und investieren Sie in die Weiterbildung Ihrer Mitarbeiter.
- **Bauen Sie einen integrierten Governance-Rahmen auf.** Entwickeln Sie eine klare Governance-Struktur, die etablierte Standards für Business Continuity (ISO 22301), Notfall-/Krisenmanagement (ISO 22320/ISO 22361), IT Service Continuity (ISO/IEC 27031) und KI-Management (ISO/IEC 42001) abdeckt und ethische Fragen proaktiv adressiert.

Organisationen, die diesen Weg einschlagen, werden nicht nur unvorhergesehene Ereignisse besser bewältigen. Sie werden die Fähigkeit entwickeln, Unsicherheit in einen strategischen Vorteil zu transformieren. Intelligente Resilienz ist ein Schlüsselfaktor für die Zukunftsfähigkeit.

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



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

Stand: Februar 2026

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 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/useng ; S. 3: iStock.com/robuart; S. 5: iStock.com/Nuthawut Somsuk; S. 7: iStock.com/Rudzhan Nagiev; S. 9: iStock.com/stock_shoppe; S. 13: iStock.com/Yayasya; S. 16: iStock.com/metamorworks

© Copyright Controllit AG