

WebKonferenz der IT-Sicherheit "BCM/BACKUP" am 09. Juni 2026

Modulares BCM für resiliente Organisationen

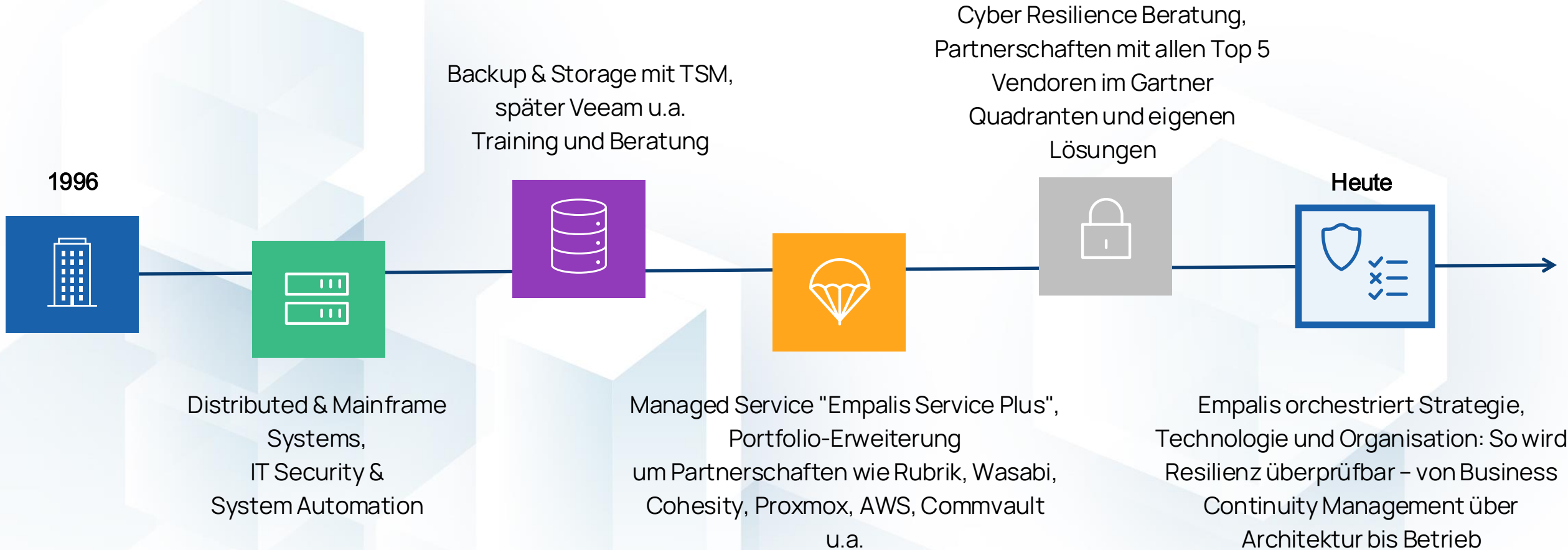
Cyber Resilience, BCM und Backup strategisch verbinden – von der reinen Datensicherung zur nachweisbaren Resilienz

Michael Melcher, Senior-Consultant Empalis Consulting GmbH

09.062026



Resilienter mit Empalis



So wird Business Resilienz einfach und belastbar auditfähig

Wir orchestrieren Strategie, Technologie und Organisation für Sie

Sie wählen den Einstiegspunkt. Wir unterstützen Sie bei Analyse, Umsetzung und Nachweisbarkeit – abgestimmt auf Reifegrad, Ressourcen und regulatorische Anforderungen.

So wird Resilienz überprüfbar – von Business Continuity Management über Architektur bis Betrieb.

- Wir reduzieren Komplexität und schaffen Transparenz.
- Wir managen Ihre Themen – von BCM und Risiko über Governance bis Recovery: fachlich, regulatorisch und technisch.
- Sicher, verlässlich und einfach zu handhaben.



Die Realität 2026



„Wie schnell werden wir wieder handlungsfähig?“

Cyberangriffe

Häufigkeit und Komplexität steigen kontinuierlich.

Regulatorischer Druck

NIS2, DORA und weitere Vorgaben fordern Nachweisbarkeit.

Cloud-Abhängigkeiten

Hybride Umgebungen erhöhen die Recovery-Komplexität.

Fachkräftemangel

Krisenreaktionsfähigkeit leidet unter Ressourcenknappheit.

Backup ≠ Resilienz



Warum klassische Backup-Konzepte nicht mehr ausreichen

- Datensicherung allein stellt keine Betriebsfähigkeit sicher
- Fehlende Recovery-Priorisierung verzögert den Wiederanlauf
- Keine Governance – kein klarer Verantwortlicher
- Krisenorganisation fehlt vollständig

Backup vorhanden ≠ Organisation resilient

Angreifer zielen auf den Wiederanlauf



Ransomware

Verschlüsselung ganzer Infrastrukturen – inklusive Backup-Systeme.



AD-Kompromittierung



Cloud-Angriffe

SaaS- und Cloud-Tenants werden gezielt als Einfallstor genutzt.



Angriffe auf Recovery

Regulatorischer Druck wächst



NIS2

Meldepflichten,
Mindestanforderungen,
Haftung

DORA

Digitale Betriebsstabilität
für Finanzunternehmen

Was Regulatoren fordern

- Auditierbare
Recovery-Nachweise
- Dokumentierte
Governance-
Strukturen
- Regelmäßige Tests
und Übungen

Technik allein erfüllt keine Compliance.

Typische Fehlannahmen

„Wir haben Backups.“

Backup ist kein Wiederanlaufplan.

„Cloud reicht.“

Shared Responsibility bedeutet geteilte Verantwortung – nicht vollständige Absicherung.

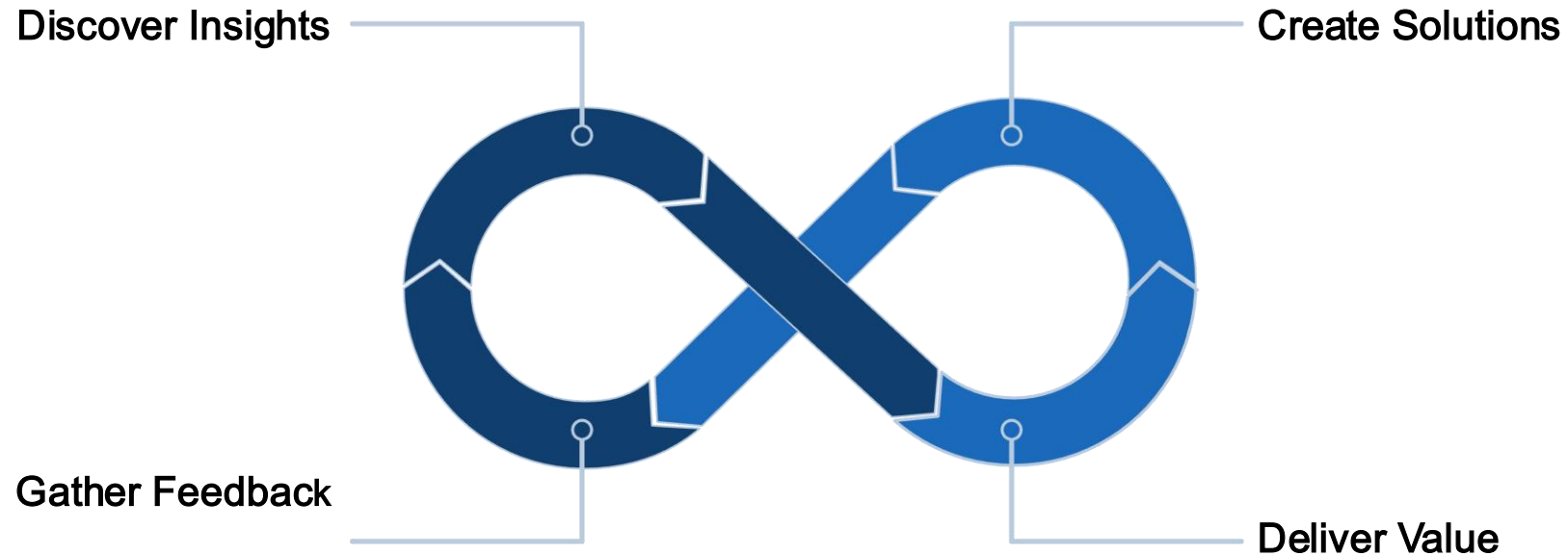
„IT kümmert sich.“

BCM ist eine Managementaufgabe, keine reine IT-Funktion.

„Recovery testen wir später.“

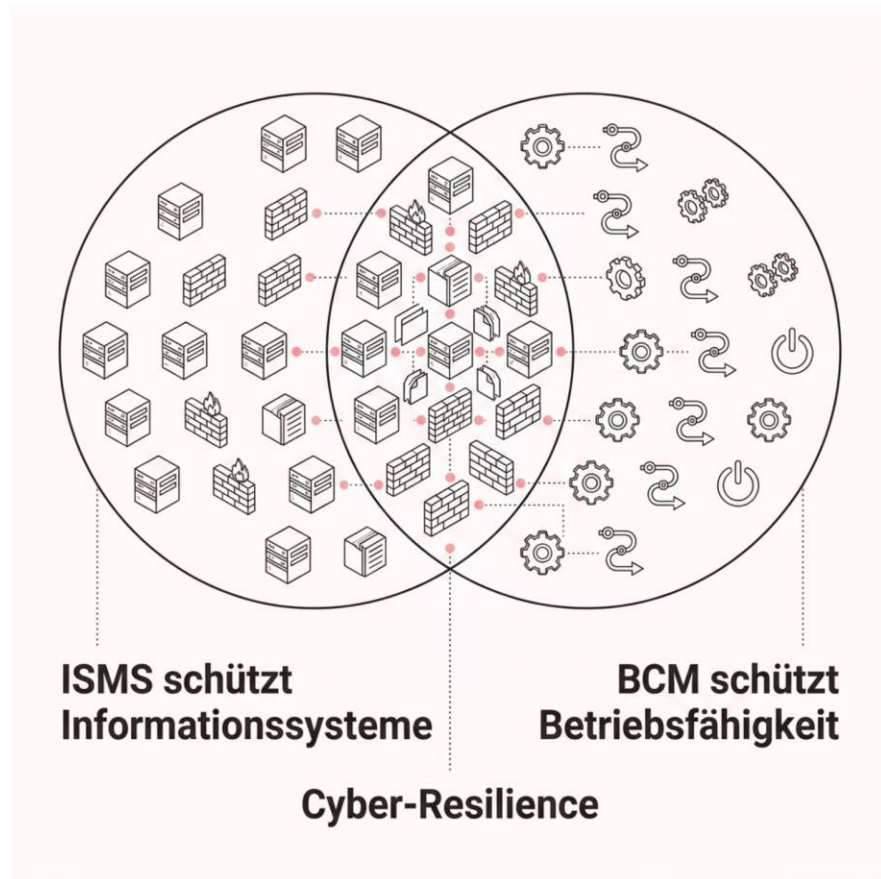
Nicht getestete Recovery bleibt Theorie.

Was BCM wirklich bedeutet



BCM schützt die Betriebsfähigkeit – nicht nur Daten. Es verbindet Governance, Krisenmanagement und technische Recovery zu einem ganzheitlichen Rahmenwerk.

ISMS und BCM gehören zusammen



Zwei Disziplinen - ein Ziel

ISMS schützt die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen.

BCM schützt die organisatorische Handlungsfähigkeit im Krisenfall.

Gemeinsam bilden sie die Grundlage echter Cyber Resilience.

Recovery wird zum kritischen Faktor



„Kontrollierte Recovery entscheidet.“

Recovery-Orchestrierung

Strukturierter, priorisierter
Wiederanlauf kritischer Systeme

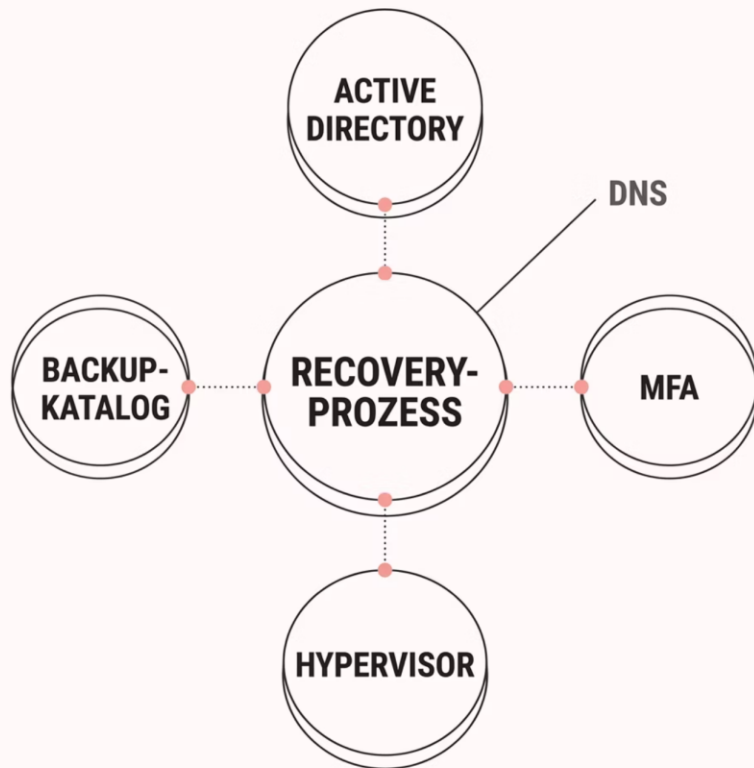
Cyber Recovery

Isolierte Wiederherstellung nach
gezielten Angriffen

Wiederanlauf

Definierte Sequenzen für Business-Continuity

Kritische Abhängigkeiten im Recovery



Warum Recovery-Konzepte oft nur theoretisch funktionieren

Viele Wiederanlaufpläne setzen Systeme voraus, die im Ernstfall selbst kompromittiert sind.

- Active Directory als Single Point of Failure
- DNS und MFA blockieren Authentifizierung
- Hypervisor und Backup-Katalog als Angriffsziele

Abhängigkeiten müssen explizit dokumentiert und getestet sein.

Typische Schwachstellen in der Praxis

Fehlende Governance

Keine klaren Verantwortlichkeiten für BCM und Recovery

Keine Übungen

Krisenszenarien werden nie realitätsnah durchgespielt

Ungetestete Recovery

Wiederanlaufpläne existieren, werden aber nie validiert

Keine Priorisierung

Alle Systeme gelten als gleich kritisch

Technologie allein reicht nicht - Governance und Prozesse sind entscheidend.

Moderne Recovery-Architekturen



Immutable Backup

Unveränderliche Sicherungskopien schützen vor Manipulation.



Zero Trust

Kein implizites Vertrauen
— auch intern nicht.



Air Gap

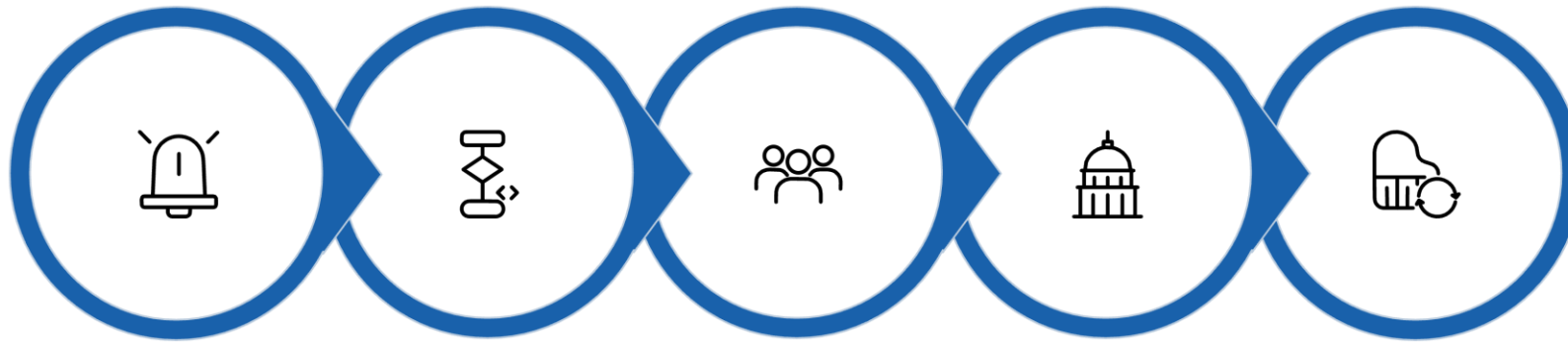
Physische oder logische Trennung verhindert Ausbreitung.



Recovery-Zonen

Dedizierte, isolierte Umgebungen für kontrollierten Wiederanlauf.

Krisenmanagement: Mehr als Technik



Vorfalls-
erkennung

Entscheidungs-
wege

Rollen &
Kommunikation

Behörden-
meldung

Wieder-
anlauf

Technik allein löst keine Krise. Klare Entscheidungswege, definierte Rollenmodelle und strukturierte Kommunikation sind ebenso entscheidend wie technische Maßnahmen.

Cloud ersetzt kein BCM



Shared Responsibility - geteilte Verantwortung

- ☁️ SaaS-Anbieter sichern Plattform – nicht Ihre Daten
- 🖨️ Tenant-Recovery liegt in der Verantwortung des Kunden
- ☁️ Multi-Cloud erhöht Komplexität und Abhängigkeiten

Cloud ersetzt kein BCM - sie erweitert dessen Anforderungen

Recovery-Tests sind Pflicht



Was getestet werden muss

- Vollständige Systemwiederanläufe
- Applikations- und Integrationstests
- Recovery-Sequenzen unter realen Bedingungen
- Krisenübungen mit Entscheidungsträgern

Nicht getestete Recovery
ist ein Geschäftsrisiko

Erst der Test beweist, dass
ein Plan funktioniert.

So entsteht nachweisbare Resilienz

Governance

Klare Verantwortung, Richtlinien, Reporting

Recovery

Technisch und organisatorisch validiert

Übungen

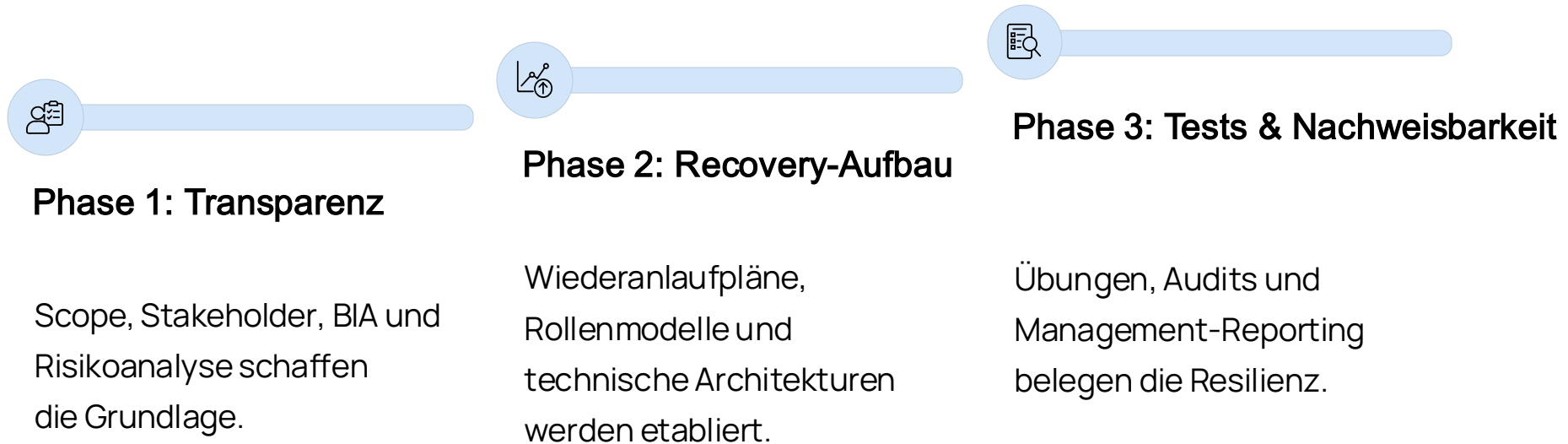
Regelmäßige Krisenszenarien und Tests

Segmentierung

Netzwerk- und Systemtrennung als Schutz

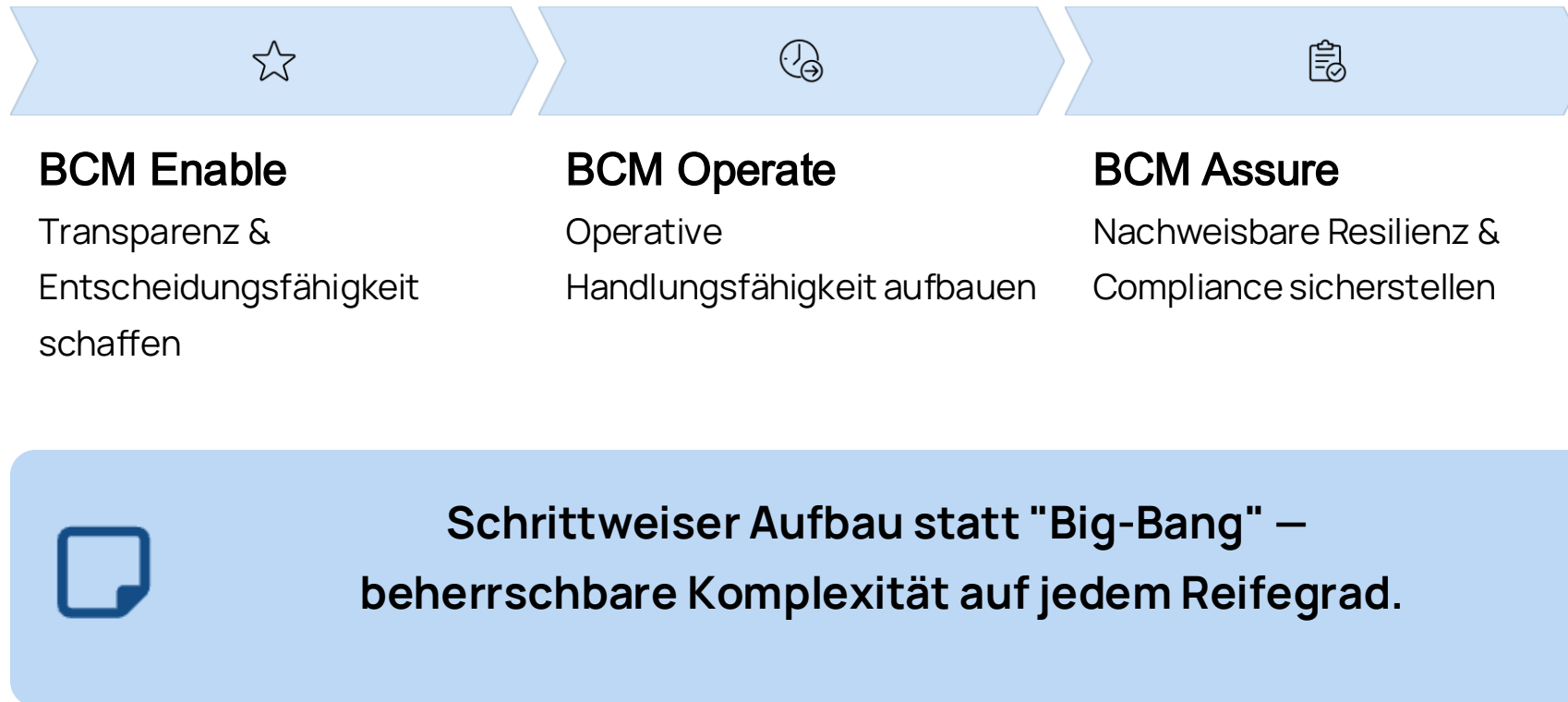
Resilienz entsteht organisatorisch und technisch.

Strukturierter Aufbau resilienter Organisationen



Resilienz entsteht schrittweise – nicht durch einen einmaligen Big-Bang-Ansatz.

Der modulare Empalis BCM-Ansatz



Warum der modulare Empalis BCM- Ansatz funktioniert



Strukturierter Einstieg

Kein überfordernder "Big-Bang" – klarer Startpunkt



Beherrschbare Komplexität

Jede Phase liefert eigenständigen Mehrwert



Kontinuierliche Verbesserung

Reifegrad wächst schrittweise und messbar



Flexible Reifegrade

Anpassbar an Unternehmensgröße und Regulatorik

Resilienz wird steuerbar - nicht zufällig.

Boost your BCM

BCM Enable

- **Ziel:** Orientierung & Entscheidungsfähigkeit schaffen

BCM Operate

- **Ziel:** Operative Handlungsfähigkeit im Notfall herstellen

BCM Assure

- **Ziel:** Nachweisbare Resilienz & Compliance sicherstellen

Empalis BCM Enable



Was BCM Enable liefert

- Scope-Definition und Stakeholder-Identifikation
- High-Level Business Impact Analysis (BIA)
- Risikoanalyse kritischer Prozesse
- Management-Readout und Priorisierung

BCM beginnt mit Transparenz – über Abhängigkeiten, Risiken und Verantwortlichkeiten

Empalis BCM Operate



Recovery muss organisatorisch und technisch funktionieren.

Was BCM Operate liefert



Detail-BIA & Prozessanalyse

Kritische Prozesse und IT-Abhängigkeiten vollständig kartieren



Wiederaanlaufpläne & Notfallhandbuch

Praxistaugliche Runbooks für alle kritischen Szenarien



Rollenmodell

Klare Verantwortlichkeiten für Krisenfall und Recovery

Empalis BCM Assure



Was BCM Assure liefert

- Regelmäßige Recovery-Tests und Krisenübungen
- Dokumentierte Szenarien und Testergebnisse
- Auditfähige Nachweise für Regulatoren
- Management-Reporting und KPI-Tracking

Nicht getestete Resilienz bleibt Theorie.

Warum BCM mit Empalis



Unsere Stärken als Resilience-Partner

-  Tiefe Recovery-Erfahrung aus realen Kriseneinsätzen
-  Verbindung von Security, Governance und Backup-Expertise
-  Cyber-Recovery und Betriebs-Know-how aus einer Hand

Nicht nur Datensicherung - sondern kontrollierte Wiederanlauffähigkeit.

Die wichtigsten Erkenntnisse

Backup allein reicht nicht

Datensicherung ist
Voraussetzung, nicht Lösung.

Recovery muss getestet werden

Ungetestete Pläne sind kein Schutz.

BCM verbindet Business & IT

Resilienz ist eine
Managementaufgabe.

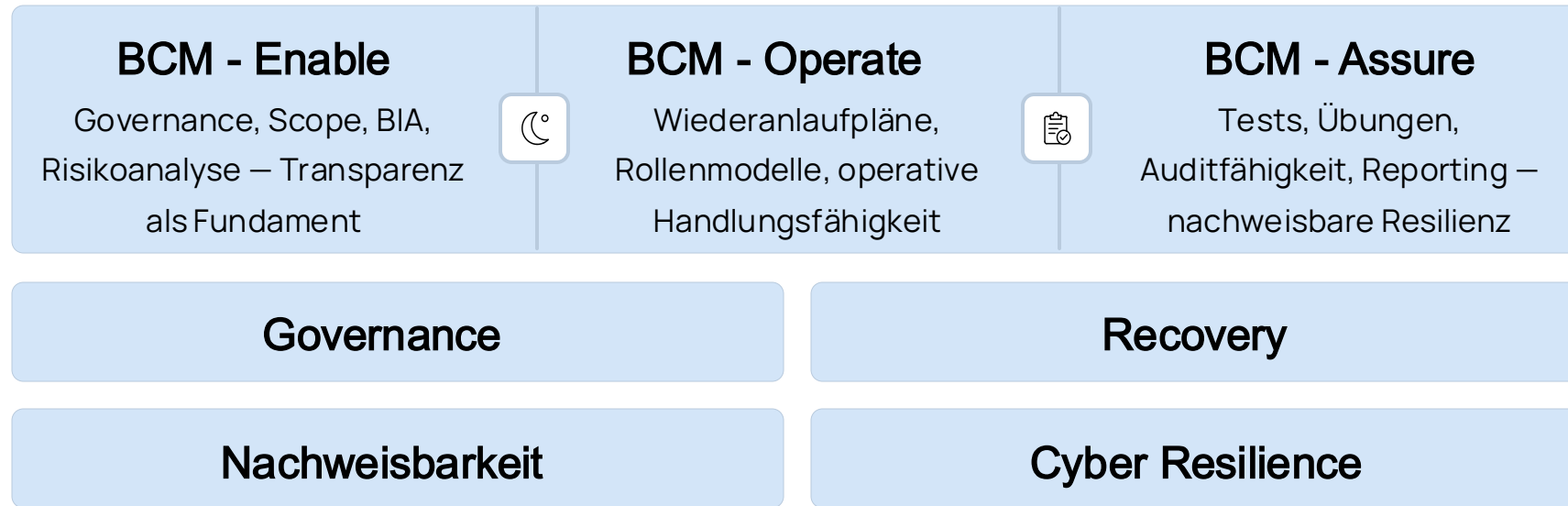
Governance wird kritisch

NIS2 und DORA fordern Nachweisbarkeit.

Resilienz entsteht organisatorisch UND technisch

Beide Dimensionen müssen zusammenwirken.

Empalis BCM - auf einen Blick



Empalis BCM-Workshops



**Wie belastbar sind
Ihre Recovery-
Prozesse heute?**

Wann wurde zuletzt ein
vollständiger
Wiederanlauf getestet?

**Wo liegen typische
Schwachstellen?**

Governance, Technik
oder organisatorische
Handlungsfähigkeit?

Wie verbindet man BCM und Recovery sinnvoll?

Welche Schritte sind in Ihrer Organisation realistisch?

Vielen Dank



„Resilienz entsteht nicht durch einzelne Technologien, sondern durch Governance, Recovery-Fähigkeit und getestete Prozesse.“

Individuellen Termin vereinbaren

✓ Ich wünsche eine Demo von einem spezifischen Produkt (30 Minuten Vorgespräch) - Produktauswahl

Viking 365

Sie möchten mehr über unsere Viking Lösung zur Sicherung von M365 Daten lernen.

Viking Backup Guardian

Sie möchten mehr über unsere cyberresiliente Backup as a Service Lösung für all Ihre Workloads lernen.

 Veeam Data Platform

Sie wünschen einen Überblick über die Data-Resilience Lösung unseres Partners Veeam.

Welche Fragen sind für Sie noch offen geblieben? Vereinbaren Sie gern mit uns einen unverbindlichen

Termin: <https://www.empalis.de/kontakt/termin-vereinbaren/>



*Wir geben volle Power
für Ihre Daten.*

Herzlichen Dank für Ihre Aufmerksamkeit!

Michael Melcher

Data Protection Consulting

Mobil: +49 160 98526034

E-Mail: michael.melcher@empalis.com

