

Ratgeber: Business Continuity Management



ANMATHO AG

VORWORT

Als Expertin für Business Continuity Management (BCM) bin ich überzeugt: In einer Welt voller Unsicherheiten schützt ein vorausschauendes BCM nicht nur Ihre Geschäftsprozesse, sondern letztlich die Existenz Ihres Unternehmens. BCM schafft Klarheit darüber, was im Ernstfall zählt, sichert Handlungsfähigkeit unter Druck und bewahrt Ihr Unternehmen vor gravierenden finanziellen Verlusten, Imageschäden oder regulatorischen Konsequenzen.

Ein praxisnahes Beispiel: Bei einer Hochwasserkatastrophe kommt es in mehreren Regionen zu einem vollständigen Ausfall der Strom- und Gasversorgung. Um auf ein solches Ereignis reagieren zu können sind bereits im Vorfeld alle kritischen Prozesse und Ressourcen im Rahmen einer Business Impact Analyse (BIA) zu identifizieren, unter anderem die Leit- und Steuerungstechnik der Strom- und Gasnetze sowie die Kommunikations- und IT-Infrastruktur. Für alle versorgungsrelevanten Bereiche sind Notfallpläne inklusive klar definierter Verantwortlichkeiten, alternativer Kommunikationswege und mobiler Notstromversorgung zu erstellen.

Während der Krise sind die vorbereiteten Notfallmaßnahmen zu aktivieren: Mitarbeitende setzen lokale Aggregate zur Notstromversorgung der Steuerzentralen ein, alternative Kommunikationsmittel kommen zum Einsatz und das Krisenteam koordiniert die Wiederherstellung beschädigter Infrastrukturen. Dadurch gelingt es, die Energieversorgung von Krankenhäusern, Wasserwerken und anderen systemrelevanten Einrichtungen trotz der massiven Störung rasch wiederherzustellen und einen längeren Blackout zu verhindern.

In Zeiten wachsender Risiken ist BCM kein „nice-to-have“, sondern die Grundlage für nachhaltige Resilienz, gesichertes Vertrauen bei Kunden und Partnern und die Erfüllung Ihrer Sorgfaltspflichten als Führungskraft. Nutzen Sie diesen Leitfaden, um Ihr Unternehmen krisenfest und zukunftssicher aufzustellen – bevor der Ernstfall eintritt.



„BCM schafft Klarheit darüber, was im Ernstfall zählt.“

Sandra Cleven

(Beraterin für Informationssicherheit, Datenschutz und Business Continuity Managerin)

INHALT

EINFÜHRUNG	4
GRUNDLAGEN UND BEGRIFFSABGRENZUNGEN	5
AUFBAU UND ORGANISATION	7
RISIKOMANAGEMENT	8
BUSINESS IMPACT ANALYSE (BIA)	9
NOTFALLMANAGEMENT UND WIEDERANLAUFPLANUNG	10
TESTS, ÜBUNGEN, SCHULUNGEN UND KONTINUIERLICHE VERBESSERUNG	11
INTEGRATION UND OPTIMIERUNG	12
WEITERFÜHRENDE INFORMATIONEN	13

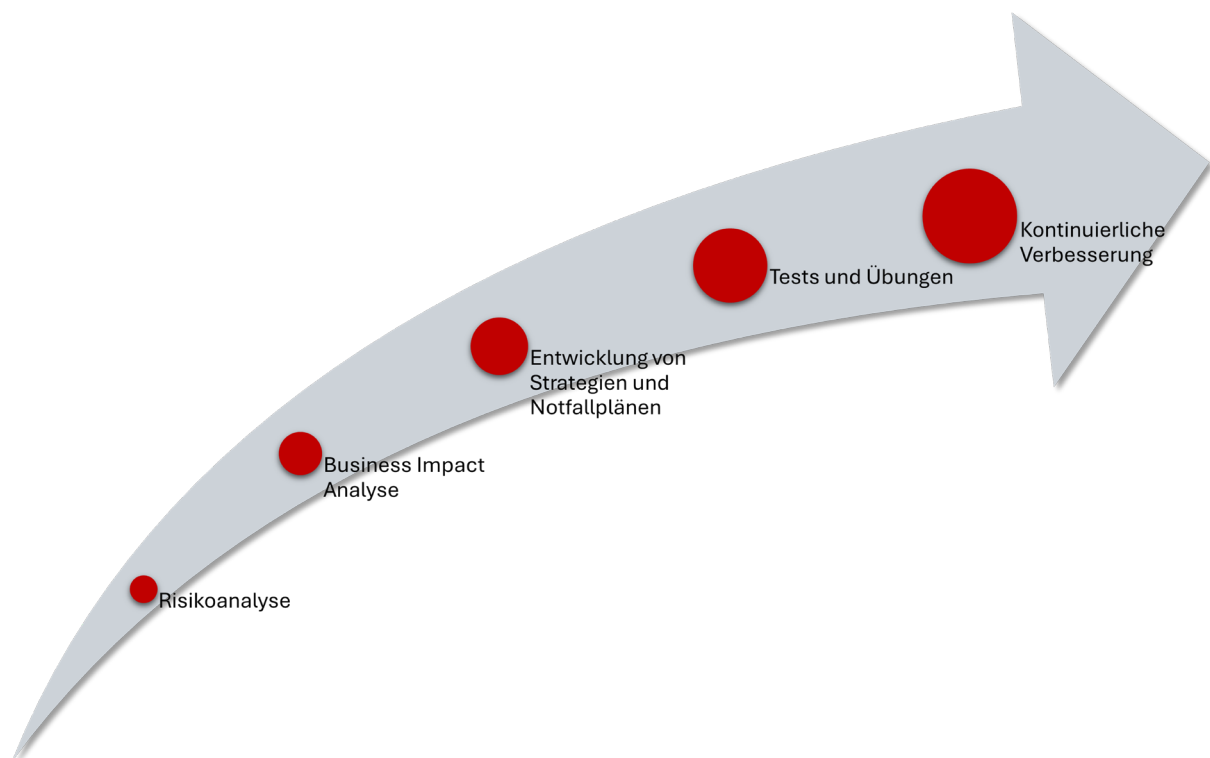
Business Continuity Management (BCM) sorgt dafür, dass Ihr Unternehmen auch im Krisenfall handlungsfähig bleibt und seine entscheidenden Geschäftsprozesse abgesichert sind. Ziel eines BCM ist es, Störungen vorzubeugen, Schäden im Ereignisfall zu minimieren und den Geschäftsbetrieb rasch wiederherzustellen.

Bedeutung für Unternehmen:

Für Unternehmen bedeutet ein funktionierendes BCM nicht nur die Sicherung ihrer Existenz und ihres Rufes, sondern auch eine Reduktion finanzieller Verluste und die Einhaltung gesetzlicher Vorgaben. Durch strukturierte Analysen und Prozesse gewinnen Sie Transparenz über Abläufe und stärken die Resilienz Ihres Unternehmens.

Der BCM-Lebenszyklus:

Der BCM-Lebenszyklus führt in mehreren Schritten von der Risikoanalyse über die Business Impact Analyse zur Entwicklung von Strategien und Notfallplänen, deren regelmäßiger Test und fortlaufende Verbesserung einen wirksamen Schutz gewährleisten. Ein etabliertes BCM ist damit keine einmalige Aktion, sondern ein kontinuierlicher Managementprozess für nachhaltige Sicherheit und Zukunftsfähigkeit Ihres Unternehmens



GRUNDLAGEN UND BEGRIFFSABGRENZUNGEN



Dieser Abschnitt soll den Einstieg in das Themenfeld Business Continuity Management erleichtern, indem zentrale Begriffe verständlich voneinander abgegrenzt werden.

Business Continuity Management

Business Continuity Management (BCM) bezeichnet den ganzheitlichen Ansatz, unternehmenskritische Geschäftsprozesse dauerhaft abzusichern und in Krisen- oder Notfallsituationen deren Fortführung oder schnellstmögliche Wiederherstellung zu gewährleisten. BCM umfasst die Planung, Steuerung sowie kontinuierliche Verbesserung eines Systems von Maßnahmen, die Risiken adressieren und die organisatorische Resilienz stärken. Grundlage aller Maßnahmen ist dabei der Lebenszyklus nach dem PDCA-Prinzip („Plan-Do-Check-Act“).

Notfallmanagement

Notfallmanagement beschreibt die organisatorische, technische und personelle Vorbereitung auf spezifische gravierende Störungen (z. B. Brand, IT-Ausfall) mit dem Ziel, Schäden zu begrenzen und den geordneten Übergang in den Wiederanlauf zu ermöglichen. Notfallmanagement ist Teil des übergeordneten BCM und konkretisiert, was im Ernstfall zu tun ist (Notfallpläne, Sofortmaßnahmen).

Krisenmanagement

Krisenmanagement bezieht sich auf die Steuerung außergewöhnlicher, meist unvorhersehbarer Ereignisse, die das Unternehmen in seiner Existenz bedrohen. Es umfasst die kurzfristige Entscheidungs- und Kommunikationsfähigkeit bis hin zur Leitung von Krisenstäben. Krisenmanagement agiert oft, wenn bestehende Notfallpläne nicht mehr ausreichen und erfordert erweiterte strategische Steuerung.

Risikomanagement

Risikomanagement ist der kontinuierliche Prozess, alle relevanten Risiken systematisch zu identifizieren, zu bewerten und zu steuern, um unerwünschte Ereignisse zu vermeiden oder deren Auswirkungen zu begrenzen. Es ist eng mit BCM verzahnt, geht aber grundsätzlich weiter, da es nicht nur existenzielle Risiken, sondern auch alltägliche operative Risiken betrachtet. BCM konzentriert sich insbesondere auf existenzbedrohende Risiken mit Bezug auf Geschäftsprozesse und Ressourcen.

Business Impact Analyse (BIA)

Die Business Impact Analyse (BIA) ist ein Kernelement des BCM. Sie bewertet systematisch, welche Geschäftsprozesse und Ressourcen für das Unternehmen besonders kritisch sind und welche Folgen deren Ausfall hätte. Anders als das Risikomanagement konzentriert sich die BIA nicht auf Ursachen, sondern auf die Auswirkungen – etwa finanzielle Verluste, Reputationsschäden oder rechtliche Konsequenzen. Die Ergebnisse der BIA bilden die Grundlage, um Notfallmaßnahmen und Wiederherstellungspläne gezielt auf jene Bereiche auszurichten, deren Ausfall das Unternehmen am stärksten gefährden würde.

GRUNDLAGEN UND BEGRIFFSAB- GRENZUNGEN



Einordnung im Kontext von ISMS, Datenschutz und Compliance:

BCM ist eng mit anderen Managementsystemen wie dem Informationssicherheits-Managementsystem (ISMS, z.B. nach ISO 27001) und dem Datenschutzmanagement verbunden. Während das ISMS sich um Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Systemen kümmert, erweitert BCM den Fokus auf die ganzheitliche organisatorische Betriebsfähigkeit. Datenschutzanforderungen (z. B. laut DSGVO) spielen eine Rolle, wenn personenbezogene Daten in Notfallmaßnahmen oder Wiederherstellungsprozessen verarbeitet werden. Compliance-Anforderungen beziehen sich auf die Einhaltung gesetzlicher, branchenspezifischer und vertraglicher Vorgaben (z. B. Organisationspflichten, Meldepflichten bei Vorfällen).

Überblick zu regulatorischen und gesetzlichen Vorgaben:

Die Ausgestaltung und Notwendigkeit eines BCM wird zunehmend durch gesetzliche und regulatorische Anforderungen bestimmt. Zu den wichtigsten Rahmenwerken zählen:

- ISO 22301: International anerkannter Standard für BCM-Systeme
- BSI-Standard 200-4: Leitlinie speziell für deutsche Organisationen/Behörden
- IT-Sicherheitsgesetz, KRITIS-Verordnung: Vorgaben für Betreiber Kritischer Infrastrukturen
- Datenschutz-Grundverordnung (DSGVO): Reaktionspflichten bei Datenverlusten
- Branchenspezifische Aufsichtsanforderungen, z. B. MaRisk für Banken und Versicherungen

Unternehmen profitieren durch die abgestimmte Umsetzung von BCM, Notfallmanagement und Risikomanagement und sichern so nicht nur ihren betrieblichen Fortbestand, sondern auch die Einhaltung rechtlicher und regulatorischer Pflichten.



AUFBAU UND ORGANISATION



Aufbau und Organisation des BCM:

Der Aufbau und die Organisation eines wirksamen Business Continuity Managements (BCM) folgen klar definierten Strukturen und Prozessen, um eine effektive Vorbereitung, Reaktion und Wiederherstellung im Krisenfall sicherzustellen.

Projektmanagement und Aufbau der BCM-Organisation

Zu Beginn empfiehlt es sich, das BCM als eigenes Projekt aufzusetzen und ein dediziertes Projektteam zu bestimmen. Zentrale Aufgabe ist dabei der Aufbau einer BCM-Organisation mit klaren Rollen und Verantwortlichkeiten: Die Geschäftsleitung trägt die Gesamtverantwortung, benennt einen zentralen BCM-Beauftragten (oft „Business Continuity Manager“ genannt), der das Vorhaben koordiniert und die Implementierungsmaßnahmen steuert. So wird eine klare Führungsstruktur geschaffen, die Durchsetzungskraft und Ressourcen garantiert.

Beispiel: Ein Unternehmen richtet einen BCM-Lenungskreis ein, der aus dem BCM-Beauftragten, der IT-Leitung und den Leitungen kritischer Geschäftsbereiche besteht.

Einbindung relevanter Abteilungen

Effektives BCM lebt von der abteilungsübergreifenden Zusammenarbeit: Die Integration aller relevanten Bereiche – etwa IT, Facility Management, Personal, Produktion, Einkauf und Kommunikation – stellt sicher, dass das BCM nicht isoliert bleibt, sondern die gesamte betriebliche Wertschöpfungskette abdeckt. Jede Abteilung bringt spezifisches Fachwissen und realistische Szenarien ein, was die Belastbarkeit der Notfallpläne steigert.

Beispiel: In Workshops entwickelt jede Abteilung eine Übersicht kritischer Abläufe und ressourcenbezogener Abhängigkeiten.

Rollen, Verantwortlichkeiten und Einbindung der Geschäftsleitung

Die Rollenverteilung ist essenziell für die Handlungsfähigkeit im Notfall:

- **Geschäftsleitung:** Gibt die strategische Richtung vor, entscheidet über zentrale Maßnahmen und stellt Ressourcen bereit.
- **BCM-Beauftragter:** Koordiniert alle BCM-Aktivitäten, wirkt als Schnittstelle zwischen Management und Fachabteilungen und überwacht den Fortschritt.
- **Fachbereichsverantwortliche:** Steuern die Umsetzung der BCM-Prozesse in ihren jeweiligen Bereichen, identifizieren kritische Prozesse und stellen die Pflege der Notfallpläne sicher.

Beispiel: Die IT übernimmt die Verantwortung für die Notfallwiederherstellung von IT-Systemen, das Facility Management entwickelt Notfallkonzepte für Gebäude.

Kommunikation und Bewusstseinsbildung

Nachhaltiger Erfolg im BCM setzt auf eine starke Kommunikation und Sensibilisierung der Mitarbeitenden. Transparente Informationsflüsse – etwa über Kick-off-Meetings, regelmäßige Schulungen, Übungen und interne Kampagnen – fördern das Verständnis und Engagement im gesamten Unternehmen. Eine festgelegte Kommunikationsstruktur, auch für den Krisenfall, stellt sicher, dass im Notfall jeder weiß, was zu tun ist und wen er informiert.

Beispiel: Ein jährlicher BCM-Tag mit Simulationen und Vorträgen vermittelt Notfallroutinen und erhöht die Akzeptanz für BCM-Maßnahmen.

Durch eine gezielte Projektorganisation, klare Zuweisung von Verantwortlichkeiten, die Einbindung aller wichtigen Abteilungen und kontinuierliche Kommunikation entsteht eine belastbare BCM-Struktur, die das Unternehmen effizient auf Störungen vorbereitet und die Widerstandsfähigkeit nachhaltig sichert.



Ein wirksames Risikomanagement ist ein zentraler Pfeiler des Business Continuity Managements (BCM) und sichert den nachhaltigen Fortbestand eines Unternehmens gegen interne und externe Bedrohungen ab.

1. Grundlagen des Risikomanagements

Risikomanagement im BCM ist der strukturierte Prozess, um potenzielle Risiken – also Ereignisse oder Entwicklungen, die den Geschäftsbetrieb stören oder lahmlegen könnten – frühzeitig zu erkennen, zu bewerten und geeignete Gegenmaßnahmen zu planen. Typische Risiken sind zum Beispiel Cyberangriffe, Naturkatastrophen, Lieferantenausfälle oder auch technische Defekte. Anders als das Krisenmanagement liegt der Fokus auf vorbeugenden, vorausschauenden Maßnahmen, um Schäden zu verhindern oder zumindest zu begrenzen.

3. Risikominderungsmaßnahmen und Priorisierung

Auf Basis der Bewertung erfolgt die Entwicklung und Umsetzung von Maßnahmen zur Risikominderung. Vorrangig sind Risiken zu adressieren, deren Kombination aus Eintrittswahrscheinlichkeit und Schadensausmaß besonders hoch ist. Mögliche Maßnahmen reichen von technischen Lösungen (z. B. Notfall-Stromversorgung, Firewalls, redundante IT-Systeme) über organisatorische Vorkehrungen (z. B. Notfallpläne, Lieferantenmanagement) bis zu Schulungen der Mitarbeitenden.

Beispiel: Das oben identifizierte Stromausfall-Risiko wird durch die Installation einer unterbrechungsfreien Stromversorgung (USV) und die Anpassung des Notfallplans reduziert.

2. Identifikation, Analyse und Bewertung von Risiken

Der erste Schritt besteht darin, die relevanten Risiken systematisch zu erfassen. Dies gelingt etwa durch Workshops mit Fachbereichen, Auswertung von Schadenshistorien und Recherchen zu branchenspezifischen Gefahren. Anschließend werden die Risiken hinsichtlich ihrer Wahrscheinlichkeit und der Schwere möglicher Auswirkungen bewertet, häufig anhand einer Risikomatrix (z. B. 1-5 für Eintrittswahrscheinlichkeit und Schadenhöhe).

Beispiel: In einem Logistikunternehmen wird das Risiko „Stromausfall am zentralen Standort“ identifiziert. Die Eintrittswahrscheinlichkeit wird als mittel eingeschätzt, aber der potenzielle Schaden als existenzbedrohend.

4. Risikomanagement nach ISO 27005 und BSI 200-3

International anerkannte Standards wie ISO 27005 und der BSI-Standard 200-3/200-4 bieten strukturierte Methoden und Vorgaben, um Risiken im Unternehmen zu identifizieren, zu bewerten, zu behandeln und zu überwachen. Die ISO 27005 fokussiert auf die Informationssicherheit, ist durch ihre Prozesse (z. B. Risikoidentifikation, -bewertung, -behandlung, -akzeptanz und Monitoring) aber auch als Vorlage für das BCM nutzbar. Der BSI 200-3 ist speziell für den deutschen Kontext relevant und bietet einheitliche Definitionen, Risikoanalyseschritte sowie ein abgestimmtes Zusammenspiel mit anderen Managementsystemen wie dem IT-Grundschutz.

Praxis-Tipp:

Führen Sie regelmäßige Risiko-Workshops mit Vertretern aller Geschäftsbereiche durch. Nutzen Sie Checklisten und bewährte Szenarien aus Standards wie dem BSI 200-3, um Lücken in bisherigen Risikobetrachtungen zu identifizieren und Maßnahmen auf den neuesten Stand zu bringen.

Als Beratungsunternehmen bieten wir Ihnen hier vielfache Unterstützungsmöglichkeiten - sprechen Sie uns an.

BUSINESS IMPACT ANALYSE (BIA)



Die Business Impact Analysis (BIA) ist ein zentrales Werkzeug im Business Continuity Management, um gezielt herauszufinden, welche Geschäftsprozesse und Ressourcen für den Unternehmenserfolg besonders kritisch sind und welche Auswirkungen deren Ausfall hätte. Sie bildet das Fundament einer wirksamen Notfallvorsorge und hilft, Prioritäten für die Wiederherstellung und Ressourceneinsatz im Krisenfall sachlich zu begründen.

Ziele und Methodik der BIA:

Das Hauptziel der BIA ist es, die Auswirkungen möglicher Ausfälle von Geschäftsprozessen zu bewerten—finanziell, rechtlich, reputativ und operativ. Die Methodik ist systematisch und baut darauf auf, zunächst alle Kernprozesse und deren Abhängigkeiten zu erfassen. Daraufhin werden die Konsequenzen verschiedener Ausfallszenarien analysiert. Hierzu gehören Interviews und Workshops mit den Fachbereichen, die auf Prozesszuordnungen, Ressourcenlisten und die Simulation von Ausfallfällen basieren. Für jeden Prozess wird ermittelt, wie stark und in welchem Zeitraum dessen Ausfall das Unternehmen beeinträchtigen würde.

Identifikation kritischer Geschäftsprozesse und Ressourcen:

Im ersten Schritt werden alle Geschäftsprozesse und deren abhängige Ressourcen (Personal, IT-Systeme, Lieferanten, Daten etc.) strukturiert erfasst. Die Konzentration liegt auf den Prozessen, deren Unterbrechung einen besonders hohen oder existenzbedrohenden Schaden verursachen würde. Die Identifikation erfolgt oft in enger Abstimmung mit den Abteilungsleitern und dem Management.

Beispiel: Im Handel wären dies z. B. die Bestell- und Zahlungsabwicklung, im Krankenhaus die Stromversorgung und Patientenversorgung, in der Produktion die Lieferkette zentraler Komponenten.

Bewertung der Auswirkungen:

Die Auswirkungen eines Prozessausfalls werden typischerweise nach den Kriterien finanzieller Schaden (z. B. Umsatzverluste, Vertragsstrafen), rechtliche Folgen (z. B. Verstöße gegen gesetzliche Fristen oder Compliance-Anforderungen), Reputationsrisiko (z. B. negatives Medienecho, Kundenvertrauensverlust) und betriebliche Konsequenzen (z. B. Produktivitätseinbruch, Personalengpässe) eingestuft. Die Bewertung erfolgt meist anhand von Skalen (hoch/mittel/niedrig oder numerisch) und Zeithorizonten für den Eintritt von Schäden.

Beispiel: Der Ausfall der Rechnungsstellung wird mit „hohem finanziellem Schaden nach maximal 24h“ bewertet, weil dann die Liquidität gefährdet ist.

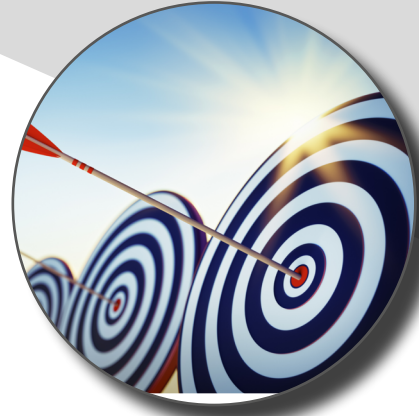
Bestimmung von MTPD, RTO und RPO:

- Die **Maximal tolerierbare Ausfallzeit (MTPD)** bezeichnet den Zeitraum, in dem ein Prozess maximal unterbrochen sein darf, bevor der Schaden für das Unternehmen nicht mehr verkraftbar ist.
- Der **Recovery Time Objective (RTO)** bestimmt, wie schnell ein Prozess nach Ausfall spätestens wieder funktionieren muss.
- Das **Recovery Point Objective (RPO)** gibt an, wie aktuell die wiederherzustellenden Daten mindestens sein müssen.

Beispiel: Im Online-Handel sind MTPD und RTO für die Bestellannahme oft nur wenige Stunden, das RPO für Kundendaten ggf. bei 15 Minuten. Demnach müssen auch die Backupzeiten diese Vorgaben widerspiegeln.



BUSINESS IMPACT ANALYSE (BIA)



Empfehlungen:

- Beziehen Sie alle relevanten Fachbereiche aktiv in die Analyse ein, um Fachwissen und Praxisnähe zu sichern.
- Nutzen Sie strukturierte Interviewleitfäden, Checklisten und standardisierte Bewertungsskalen, um die Nachvollziehbarkeit und Vergleichbarkeit Ihrer Ergebnisse zu erhöhen.
- Überarbeiten Sie die BIA regelmäßig, insbesondere nach organisatorischen oder technischen Änderungen, und stimmen Sie die Ergebnisse mit IT- und Notfallplänen ab, um wirklichen Geschäftsschutz zu erreichen.

Die BIA liefert so ein klar priorisiertes Bild aller kritischen Prozesse und ermöglicht es, Ressourcen gezielt in Notfallvorsorge und Wiederanlaufmaßnahmen zu investieren.



NOTFALLMANAGEMENT UND WIEDERANLAUFPLANUNG



Ein wirksames Notfallmanagement und eine durchdachte Wiederanlaufplanung sind entscheidend, um im Krisenfall schnell, strukturiert und zielgerichtet zu handeln und den Geschäftsbetrieb soweit möglich aufrechtzuerhalten bzw. rasch wiederherzustellen.

Entwicklung und Dokumentation von Notfallplänen

Notfallpläne legen fest, wie im Ernstfall zu reagieren ist. Sie werden auf Basis der Risikobewertung und der Business Impact Analyse individuell für die spezifischen Risiken und Prozesse eines Unternehmens entwickelt. Ein Notfallplan beschreibt unter anderem:

- Auslöser und Szenarien (z. B. Brand, IT-Ausfall, Cyberangriff)
- Sofortmaßnahmen zur Schadenbegrenzung
- Wiederherstellungsmaßnahmen und alternative Abläufe

Wichtig ist die nachvollziehbare und aktuelle Dokumentation, etwa als Notfallhandbuch oder elektronischer Leitfaden, der allen Beteiligten im Ernstfall zugänglich ist.

Beispiel: Unternehmen erstellen einen detaillierten Notfallplan für den Ausfall des Rechenzentrums, der u. a. die Alarmierung, die Verantwortlichen und das Vorgehen zur Wiederherstellung der IT-Infrastruktur regelt.

Ressourcenmanagement und Wiederherstellungsstrategien

Für eine erfolgreiche Wiederanlaufplanung müssen alle notwendigen Ressourcen – Personal, Technik, Informationen, alternative Arbeitsplätze – identifiziert und im Plan hinterlegt werden. Zentrale Fragen sind: Welche Ressourcen werden im Notbetrieb benötigt? Gibt es Alternativen, sollte etwas kurzfristig nicht verfügbar sein?

Wiederherstellungsstrategien beschreiben, wie Prozesse und Systeme so schnell wie nötig und möglich wieder einsatzfähig gemacht werden. Dazu zählen technische Lösungen (z. B. Backups, Notstrom, Ausweicharbeitsplätze) und organisatorische Maßnahmen (z. B. Bereitstellung von Schlüsselpersonal, Ersatzverfahren für ausgefallene Systeme).

Beispiel: Bei Ausfall der Hauptgeschäftsstelle wird der Betrieb innerhalb von 2 Stunden auf einen Ersatzstandort verlagert, während kritische Daten durch regelmäßige Backups rasch wiederhergestellt werden.

Definition von Verantwortlichkeiten und Abläufen

Jeder Notfallplan benennt klar die Verantwortlichen:

- Wer koordiniert (z. B. Leiter Notfallteam)?
- Wer übernimmt Kommunikation, Öffentlichkeitsarbeit, IT-Wiederherstellung, Dokumentation?

Die Definition von Rollen und Aufgaben schafft Verbindlichkeit und stellt sicher, dass Abläufe auch unter Stress funktionieren. Ein Notfallteam oder Krisenstab mit festen Stellvertretern und klar geregelter Eskalationskette ist essenziell.

Beispiel: Im Ernstfall ruft der Leiter des Notfallteams die jeweilige Einsatzleitung zusammen, ein Kommunikationsbeauftragter informiert Mitarbeitende und externe Partner nach einem vorgegebenem Kommunikationsplan.

Übergang in den Notbetrieb

Nicht immer kann die volle Geschäftstätigkeit sofort wiederhergestellt werden. Der Notbetrieb definiert Mindestanforderungen und alternative Routinen, mit denen das Unternehmen vorübergehend auf niedrigem Niveau funktioniert, bis zur vollständigen Wiederaufnahme. Die Maßnahmen helfen, existenzielle Schäden zu vermeiden und die wichtigsten Unternehmensinteressen zu wahren.

Beispiel: Nach einem schweren Stromausfall arbeitet die Buchhaltung zunächst papierbasiert weiter; Bestellungen werden telefonisch abgewickelt, bis die IT wieder verfügbar ist.

Praxisempfehlung:

Notfallpläne sollten regelmäßig getestet und geübt werden (z. B. durch Simulationen), um ihre Wirksamkeit zu überprüfen, Verantwortlichkeiten zu festigen und Schwachstellen rechtzeitig zu erkennen.

TESTS, ÜBUNGEN, SCHULUNGEN UND KONTINUIERLICHE VERBESSERUNG



Tests, Übungen, Schulungen und kontinuierliche Verbesserung sind entscheidende Säulen für die Wirksamkeit und Weiterentwicklung eines Business Continuity Managements (BCM). Sie stellen sicher, dass Notfallpläne im Ernstfall funktionieren, Mitarbeitende ihre Rollen kennen und das BCM laufend an neue Herausforderungen angepasst wird.

Planung und Durchführung von BCM-Übungen und Tests

Eine strukturierte Test- und Übungsplanung umfasst sowohl die Auswahl geeigneter Übungsarten als auch deren regelmäßige Durchführung. Hierzu zählen u. a. Desktop-Tests (Walkthroughs), Teamübungen, Simulationen sowie Vollübungen mit realitätsnahen Szenarien (z. B. Stromausfall, Cyberangriff). Ziel ist, die Funktionsfähigkeit aller Pläne, Prozesse und Ressourcen praxisnah zu überprüfen. Ein Roll-out-Plan legt Häufigkeit und Verantwortlichkeiten fest; kritische Bereiche sollten mindestens jährlich geübt werden.

Beispiel: Ein Unternehmen simuliert den Ausfall des Rechenzentrums. Mitarbeitende üben den Umschaltvorgang auf den Ersatzstandort und testen die Prozesse der Alarmierung und internen Kommunikation.

Laufende Anpassung an neue Technologien und Bedrohungen

Technologische Entwicklungen und die sich ständig ändernde Bedrohungslage (z. B. neue Cyberrisiken, Abhängigkeiten von Dienstleistern, gesetzliche Veränderungen) verlangen eine fortlaufende Überprüfung und Anpassung aller BCM-Maßnahmen. Regelmäßige Überarbeitungen der Test- und Übungspläne sowie die Integration neuer Szenarien stellen sicher, dass das BCM aktuell und belastbar bleibt.

Beispiel: Nach Einführung einer Cloud-Lösung werden eigene Testszenarien für Cloud-Ausfälle entwickelt und geübt.

Auswertung und Integration von Lessons Learned

Nach jeder Übung oder jedem Test erfolgt eine detaillierte Auswertung (z. B. in Form von Übungsprotokollen und Berichten). Dabei werden erreichte Ziele, aufgetretene Abweichungen und Verbesserungspotenziale dokumentiert. Die Integration der „Lessons Learned“ in die bestehenden Notfallpläne und Abläufe ist zentral, um Schwachstellen konsequent zu beheben.

Beispiel: Nach einer Alarmierungsübung wird deutlich, dass ein Kommunikationsverteiler veraltet war. Die Korrektur erfolgt unmittelbar, und die Kontaktliste wird fortlaufend gepflegt.

Mitarbeiterschulungen und Seminare

Ein zentraler Erfolgsfaktor im BCM ist das Wissen und die Handlungssicherheit der Mitarbeitenden. Interne Schulungen, Seminare und praktische Übungen sorgen dafür, dass alle Beteiligten im Notfall routiniert reagieren können. Dies umfasst die Einweisung in Notfallpläne, Informationspflichten sowie spezifische Rollen (z. B. Krisenteam, Kommunikation, technische Einsatzleitung).

Beispiel: In jährlichen BCM-Schulungen werden alle Schlüsselpersonen weitergebildet und durch Rollenspiele auf den Ernstfall vorbereitet.

Maßnahmen zur Schaffung eines BCM-Bewusstseins

Ein nachhaltiges BCM erfordert eine Kultur des Bewusstseins und der Achtsamkeit. Informationskampagnen, regelmäßige Erinnerungen, BCM-Tage oder interne Newsletter stärken das Verständnis und die Akzeptanz für Sicherheitsmaßnahmen. Führungskräfte und Mitarbeitende werden so regelmäßig für Risiken und Präventionsmaßnahmen sensibilisiert.

Beispiel: Der jährliche „BCM-Tag“ mit Kurzvorträgen, Simulationen und Erfahrungsberichten fördert die Identifikation mit dem Thema im gesamten Unternehmen.

INTEGRATION UND OPTIMIERUNG



Die Integration und Optimierung des Business Continuity Managements (BCM) gelingen am wirksamsten, wenn das BCM eng mit anderen zentralen Managementsystemen wie dem Informationssicherheits-Managementsystem (ISMS), Datenschutzmanagement und weiteren Compliance-Systemen verzahnt wird. Dieser integrierte Ansatz gewährleistet umfassende Resilienz, Rechtssicherheit und Effizienz.

Verzahnung mit ISMS, Datenschutz und anderen Managementsystemen

Moderne Unternehmen stehen vor der Aufgabe, nicht nur ihre Geschäftsprozesse, sondern auch ihre Informationen und personenbezogenen Daten zu schützen. Ein ISMS (z. B. nach ISO 27001) legt Schutzziele und Prozesse zur Sicherung der Vertraulichkeit, Integrität und Verfügbarkeit fest. Ein BCM ergänzt dies um die organisatorische Sicherstellung der Betriebsfähigkeit im Krisenfall. Synergien entstehen insbesondere durch:

- **Gemeinsame Risikoanalysen:** Risiken für die Informationssicherheit und Geschäftsprozesse werden zentral erfasst und bewertet, so dass Schutzmaßnahmen für beide Bereiche effektiv abgestimmt werden können.
- **Abgestimmte Notfallpläne:** Die IT-Notfallplanung bindet Vorgaben des ISMS und BCM gleichermaßen ein, um Sicherheitsvorfälle und Prozessunterbrechungen gemeinsam zu adressieren.
- **Schnittstellen zum Datenschutz:** Die DSGVO verlangt neben Vertraulichkeit auch Mindestanforderungen für Verfügbarkeit und Wiederherstellbarkeit von Daten (Art. 32, 33 DSGVO). Zentral ist das konsequente Zusammenspiel zwischen BCM und Datenschutz, z. B. durch abgestimmte Meldeprozesse und die Einbindung des Datenschutzbeauftragten in die Notfallplanung.

Beispiel: In einem Unternehmen sind die Meldefristen für Datenschutzvorfälle (DSGVO Art. 33: 72 Stunden) direkt im Alarmierungsplan des IT-Notfallmanagements hinterlegt und mit den Wiederanlaufzeiten des BCM abgestimmt. Der Datenschutzbeauftragte erhält alle Pläne, um Meldepflichten einhalten zu können.

Berücksichtigung von Anforderungen durch NIS2, ISO-Zertifizierungen u. a.

Die Anforderungen an ein BCM werden durch europäische (NIS2-Richtlinie), nationale (IT-Sicherheitsgesetz, BSI-Standards) und internationale Standards (ISO 22301, ISO 27001) weiter verschärft und konkretisiert:

- Die NIS2-Richtlinie verpflichtet Unternehmen kritischer Sektoren und digitaler Dienste zu deutlich erweiterten Vorkehrungen. Dazu zählen abgestimmte Notfallmaßnahmen, umfassende Dokumentationspflichten und verpflichtende BCM-Prozesse.
- ISO-Zertifizierungen wie ISO 22301 (BCM) und ISO 27001 (ISMS) erfordern einen systematischen Nachweis über die Integration von BCM, Informationssicherheit und Compliance. Viele Unternehmen erreichen dies durch gemeinsame Prozesse, zentrale Steuerung und konsolidierte Berichte.
- Der BSI-Standard 200-4 fördert ausdrücklich die Verzahnung von ISMS und BCM, beispielsweise durch integrierte Notfallplanungen und gemeinsam genutzte Ressourcen in der Krisenbewältigung.

Beispiel: Ein Unternehmen im Gesundheitswesen nutzt integrierte Tools, um die Anforderungen aus Datenschutz, IT-Sicherheit und BCM systematisch zu dokumentieren und regelmäßig an neue gesetzliche Vorgaben (z. B. NIS2, ISO 22301) anzupassen. So wird neben der ISO-Zertifizierung auch die Nachweispflicht gegenüber Aufsichtsbehörden gewahrt.

Empfehlung

Unternehmen sollten prüfen, inwieweit BCM, ISMS und Datenschutzmanagement bereits miteinander verzahnt sind – etwa durch integrative Risiko-Workshops, konsolidierte Pläne und abgestimmte Rollenmodelle.

WEITERFÜHRENDE INFORMATIONEN



Checklisten und Arbeitshilfen sind unerlässliche Begleiter für die effektive Einführung, Pflege und Auditing eines Business Continuity Managements (BCM). Sie bieten praxisbewährte Orientierung, helfen bei der Umsetzung von Standards und erleichtern die Dokumentation von Abläufen und Verantwortlichkeiten.

Ressourcen

- Das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** stellt im Rahmen des BSI-Standards 200-4 zahlreiche Hilfsmittel für ein BCM nach aktuellen regulatorischen Vorgaben zur Verfügung, wie etwa Formblätter für Risikoanalysen und Notfallpläne.
- **Digitale Tools** bieten zahlreiche kostenfreie Checklisten-Vorlagen für Business Continuity Pläne, die flexibel an unterschiedliche Branchenerfordernisse angepasst werden können und teilweise über eine intuitive App auch mobil bearbeitbar sind. Die Marktübersicht von KonBriefing Research listet aktuelle BCM-Software-Lösungen auf: <https://konbriefing.com/de-software/bcm/auswahl.html>

Weiterführenden Materialien auf anmatho.de

Podcasts:

- „Security on Air – Heute BCM“ (Zweiteilige Folge): Einstieg, Stolperfallen, Aufbau von BCM, Tipps aus der Praxis.
- „Security on Air – Risikobetrachtung am Beispiel Hochwasser“: Strukturierte Risikoanalyse, BIA-Anteil, Kommunikation.
- „Security on Air – BIA“. Aufbau, Tipps und Einordnung zu Risikomanagement und BCM

Blogartikel:

- „Vorgehen und Szenarien im BCM“: Praktische Schritte und Fallbeispiele zur Notfallplanung.
- „Ein Notfallmanagement systematisch einführen“: Leitfaden vom Start bis zur Übung.
- „Notfallvorsorge in der IT“: Schwerpunkt auf digitale Risiken und Wiederanlaufplanung.
- Mehrteilige Serie zum Risikomanagement im ISMS: Identifikation, Bewertung, Integration mit BCM.

Seminare:

- Business Continuity Management nach ISO 22301
- Workshops zum Risikomanagement nach ISO 27005 und BSI 200-3.
- Inhouse-Kurse und individuelle Übungsszenarien für Notfall- und Krisenmanagement.

Weiterführende Informationen unter: <https://anmatho.de/seminare/>

Diese Materialien ermöglichen eine gezielte Vertiefung der jeweiligen BCM-Teilschritte. Wenn Sie Unterstützung benötigen, sind wir gern für Sie da.

BILDRECHTE

Deckblatt: AdobeStock | 758936305 | Ekaterina

Seite 5 + 6: AdobeStock | 177435886 | pathdoc

Seite 7: AdobeStock | 1335086475 | InfiniteFlow

Seite 8: AdobeStock | 407869470 | Jo Panuwat D

Seite 9: AdobeStock | 116874347 | peterschreiber.media

Seite 10: AdobeStock | 116874347 | peterschreiber.media und AdobeStock | 1485543477 | Captain

Seite 11: AdobeStock | 512758800 | kebox

Seite 12: AdobeStock | 68271970 | blende11.photo

Seite 13: AdobeStock | 124719136 | WrightStudio

Seite 14: AdobeStock | 201306857 | onepphoto

Hinweis: Aus Gründen der besseren Lesbarkeit verzichten wir in diesem Ratgeber auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d). Die verwendeten Personenbezeichnungen beziehen sich auf alle Geschlechter.

ANMATHO AG

Winterhuder Weg 82
22085 Hamburg

info@anmatho.de

www.anmatho.de

LinkedIn: [https://www.linkedin.com/
company/anmatho-ag](https://www.linkedin.com/company/anmatho-ag)