Business Continuity & Resilienz

Schrittweise Umsetzung von BCM, ITSCM, Supplier und Vendor Continuity sowie Krisenmanagement

Eine professionelle Arbeitsbroschüre für Geschäftsleitung, Projektleitung und Fachverantwortliche. Mit Executive Management Summary, Roadmap, Leistungslandkarte, Umsetzungsschritten 1-9, Reifegrad-Checklisten, Projektpaketen und Deliverables.

RM Risk Management AG
Business-Resilienz & GRC Consultants

RM Risk Management AG, Hertistrasse 25, 8304 Wallisellen / Zürich | Tel. +41 44 360 40 40
business-continuity-resilienz.ch

Executive Management Summary

Business Continuity Management ist kein reines Dokumentationsprojekt. Es ist ein Führungsinstrument zur Sicherung kritischer Leistungen, zur Begrenzung von Schäden und zur Wiederherstellung der Handlungsfähigkeit bei Cyberangriffen, IT-Ausfällen, Gebäudeausfällen, Lieferkettenunterbrüchen, Personalausfällen oder Krisenlagen. Die Umsetzung verbindet Governance, Business Impact Analyse, Risikoanalyse, Strategie, Business Continuity Pläne, IT Service Continuity, Supplier/Vendor Continuity, Krisenmanagement, Schulung, Übungen und kontinuierliche Verbesserung.

Führung
Entscheidungen zu Risiko, Priorität und Investition

Transparenz
kritische Prozesse, Services und Abhängigkeiten

Nachweis
Pläne, Tests, Reviews und kontinuierliche Verbesserung

Management-Ziele

Die Unternehmensleitung erhält eine belastbare Entscheidungsgrundlage: Welche Leistungen sind existenziell? Welche Ausfallzeiten sind tragbar? Welche Ressourcen müssen priorisiert werden? Welche Restrisiken werden akzeptiert? Welche Investitionen sind notwendig, um Wiederanlaufziele zu erreichen? Das Ergebnis ist ein nachvollziehbares Zielbild für Resilienz, das Business, IT, Lieferanten, Kommunikation, HR, Facility Management und Krisenstab verbindet.

Umsetzungslogik

Die Broschüre strukturiert den Weg in neun Arbeitsschritte. Jeder Schritt erzeugt konkrete Ergebnisse, Freigaben und Nachweise. Dadurch entsteht eine nachvollziehbare Linie vom Managementauftrag über Analyse und Strategie bis zu umsetzbaren Plänen, Übungen und Verbesserungsmassnahmen.

Vertrauenswirkung

Ein reifes Continuity-System schafft Vertrauen gegenüber Kunden, Aufsichtsstellen, Eigentümern, Versicherern, Revisionsstellen, Lieferanten und Mitarbeitenden. Es zeigt, dass die Organisation ihre kritischen Prozesse kennt, Abhängigkeiten steuert, Krisenführung vorbereitet und die Wirksamkeit der Massnahmen regelmässig überprüft.

Erfolgsfaktoren

Erfolgreiches BCM ist schlank, priorisiert und praxisnah. Es beginnt nicht mit umfangreichen Handbüchern, sondern mit Klarheit über kritische Leistungen, Wiederanlaufanforderungen, Verantwortlichkeiten und realistische Handlungsoptionen. Entscheidend sind Management-Sponsoring, aktive Prozessverantwortliche, abgestimmte IT-Anforderungen, trainierte Krisenrollen und ein konsequentes Massnahmen-Tracking.

Management-Nutzen

Verdichtung der Ergebnisse zu Entscheidungen, Prioritäten, Investitionen, Restrisiken und Nachweisen für Geschäftsleitung und Programmsteuerung.

Beratungsansatz

Kombination aus Dokumentenreview, Interviews, Workshops, Templates, Qualitätsprüfung und pragmatischer Umsetzungsbegleitung.

Ergebnisqualität

Alle Resultate werden als nutzbare Arbeitsdokumente, Checklisten, Roadmaps und Review-Unterlagen für Betrieb, Audit und Training bereitgestellt.

Roadmap zur Umsetzung

Die Roadmap gliedert die Umsetzung in klare Phasen. Sie verhindert, dass BCM isoliert in einzelnen Fachbereichen entsteht, und sorgt dafür, dass Analyse, Strategie, Pläne, Tests und Verbesserungen logisch aufeinander aufbauen. Die Roadmap ist als Beratungsmodell, Projektstrukturplan und Management-Kommunikation einsetzbar.

1 Auftrag & Governance	2 Policy & Methodik	3 Business Impact Analyse	4 Risiko & Lagebild	5 Business Continuity Strategie	6 Business Continuity Plan	7 ITSCM & DRP	8 Supplier / Vendor Continuity	9 Übung & Review

Phase A - Initiierung und Ausrichtung

Projektauftrag, Sponsor, Scope, Rollen, Projektorganisation, Kommunikationsplan, Stakeholder, Methodik und Terminplan werden verbindlich festgelegt. In dieser Phase wird entschieden, welche Organisationseinheiten, Standorte, Prozesse, IT-Services und Lieferanten im ersten Umsetzungszyklus betrachtet werden.

Phase B - Analyse und Priorisierung

Business Impact Analyse, Service Impact Analyse, Risikoanalyse und Abhängigkeitsanalyse schaffen Transparenz. Kritische Prozesse und Services werden priorisiert, RTO/RPO-Anforderungen abgeleitet und Schwachstellen sichtbar gemacht.

Auf Basis der Analyse werden praktikable Continuity-Optionen entwickelt: Notbetrieb, manuelle Ersatzprozesse, alternative Standorte, Homeoffice, Redundanz, Backup, Ersatzlieferanten, Krisenkommunikation und Recovery-Strategien. Die Geschäftsleitung entscheidet Zielniveau, Restrisiko und Investitionsrahmen.

BCP, DRP, Supplier / Vendor Continuity Pläne, Krisenmanagement-Dokumentation, Alarmierung, Kontaktlisten, Checklisten und Wiederanlaufverfahren werden erstellt, eingeführt, trainiert und getestet. Jede Übung führt zu Lessons Learned und Massnahmen.

Management-Checkliste

- ☐ Roadmap ist durch Sponsor und Projektleitung freigegeben.
- ☐ Jeder Arbeitsschritt besitzt Ergebnis, Verantwortliche, Entscheidpunkte und Qualitätskriterien.
- ☐ Abhängigkeiten zwischen Business, IT, Lieferanten und Krisenmanagement sind explizit adressiert.
- ☐ Die Roadmap ist realistisch priorisiert und auf Quick Wins sowie Nachweise ausgerichtet.

Management-Nutzen

Verdichtung der Ergebnisse zu Entscheidungen, Prioritäten, Investitionen, Restrisiken und Nachweisen für Geschäftsleitung und Programmsteuerung.

Beratungsansatz

Kombination aus Dokumentenreview, Interviews, Workshops, Templates, Qualitätsprüfung und pragmatischer Umsetzungsbegleitung.

Ergebnisqualität

Alle Resultate werden als nutzbare Arbeitsdokumente, Checklisten, Roadmaps und Review-Unterlagen für Betrieb, Audit und Training bereitgestellt.

Leistungslandkarte

Die Leistungslandkarte zeigt, wie die Beratungsbausteine zusammenwirken. Business Continuity Management sichert kritische Geschäftsprozesse. IT Service Continuity und Disaster Recovery stellen die benötigten IT-Services wieder her. Supplier und Vendor Continuity reduzieren externe Abhängigkeiten. Krisenmanagement stellt Führungsfähigkeit, Lagebild, Kommunikation und Entscheidungsrhythmus sicher.

Business Continuity Management

BCMS-Aufbau, BCM Policy, Governance, Business Impact Analyse, Risikoanalyse, BCM-Strategie, Business Continuity Pläne, Tests, Reviews und ISO-22301-Coaching. Schwerpunkt ist die Sicherung kritischer Prozesse und Leistungen aus Sicht der Organisation.

IT Service Continuity / Disaster Recovery

SIA, Service-Mapping, Kritikalität von IT-Services, RTO/RPO-Abgleich, Recovery-Strategien, DRP, Backup-/Restore-Verfahren, technische Tests und Abstimmung mit ITSM, Informationssicherheit und Cyber-Krisenmanagement.

Supplier & Vendor Continuity

Identifikation kritischer Lieferanten und Dienstleister, Supply-Chain-Resilienz-Analyse, Risk Rating, Backup-Lieferanten, vertragliche Anforderungen, Kommunikationswege, Eskalation und Kontinuitätspläne.

Krisenmanagement, Schulung und Übungen

Krisenorganisation, Führungsmethodik, Krisenhandbuch, Lagebild, Entscheidungslogik, Kommunikationsprozesse, Schulungen, Tabletop-Übungen, Krisenstabsübungen, IT-Notfallübungen und Massnahmen-Tracking.

Projektpakete / Deliverables / Nachweise

- BCM-Rahmenwerk und Projektvorlagen
- BIA-/SIA-Ergebnisse und Kritikalitätslagebild
- BCM-, DRP-, SCP- und VCP-Pläne
- Übungsdrehbuch, Beobachtungsbogen und Lessons Learned
- Management-Review und Verbesserungs-Roadmap

Management-Nutzen

Verdichtung der Ergebnisse zu Entscheidungen, Prioritäten, Investitionen, Restrisiken und Nachweisen für Geschäftsleitung und Programmsteuerung.

Beratungsansatz

Kombination aus Dokumentenreview, Interviews, Workshops, Templates, Qualitätsprüfung und pragmatischer Umsetzungsbegleitung.

Ergebnisqualität

Alle Resultate werden als nutzbare Arbeitsdokumente, Checklisten, Roadmaps und Review-Unterlagen für Betrieb, Audit und Training bereitgestellt.

Projektauftrag, Scope & Governance

Der erste Schritt schafft Verbindlichkeit. Ohne klaren Auftrag, Sponsor, Scope und Governance bleibt BCM oft eine Sammlung einzelner Dokumente. Ziel ist ein tragfähiger Projekt- und Führungsrahmen, der Verantwortlichkeiten, Entscheidwege, Geltungsbereich, Prioritäten und Schnittstellen festlegt.

Mandat | Scope | Stakeholder | Governance | Projektplan

Ziel und Management-Fragen

Die Geschäftsleitung muss festlegen, weshalb BCM aufgebaut oder verbessert wird, welche Ziele erreicht werden sollen und welche Risiken durch das Programm reduziert werden. Geklärt werden Scope, Schutzobjekte, Standorte, Gesellschaften, kritische Leistungen, regulatorische Treiber, Kundenerwartungen und Audit-Anforderungen.

Vorgehen

In einem Kick-off werden Stakeholder, Projektrollen, Governance-Gremien, Terminplan, Kommunikationsformat, Dokumentationsstandard und Entscheidpunkte definiert. Bestehende Unterlagen wie Risikoinventar, Prozesslandkarte, Notfallpläne, IT-Dokumentation, Lieferantenlisten und Krisenmanagement-Konzepte werden gesichtet.

Qualitätskriterien

Der Auftrag ist gut, wenn Ziele messbar, Scope und Nicht-Scope transparent, Verantwortlichkeiten eindeutig und Management-Entscheide terminiert sind. BCM muss an Risiko-, Krisen-, IT-, Informationssicherheits-, Facility- und Lieferantenprozesse angebunden werden.

Ergebnisse / Deliverables

- Projektauftrag und Mandat
- Stakeholder- und Kommunikationsplan
- Scope-Matrix mit Standorten, Prozessen, Services und Gesellschaften
- Rollenmodell und Governance-Struktur
- Termin- und Entscheidungsplan

Arbeits- und Qualitätscheckliste

Prüfpunkte

- □ Sponsor und Projektleitung sind benannt und verfügbar.
- □ Scope und Prioritäten wurden auf Managementebene bestätigt.
- □ Schnittstellen zu Krisenmanagement, Risiko, IT, HR, Kommunikation, Facility und Einkauf sind definiert.
- □ Projektmethodik, Berichtswesen und Qualitätsprüfung sind freigegeben.
- □ Entscheidpunkte für Strategie, Restrisiko und Ressourcen sind eingeplant.

Reifegrad-Checkliste je Arbeitsschritt

- □ Initial: Projektauftrag, Scope & Governance ist erkannt, aber Verantwortung, Methode und Nachweise sind noch nicht verlässlich etabliert.
- □ Basis: Vorgehen, Rollen und erste Inhalte zu Projektauftrag, Scope & Governance sind dokumentiert; Qualität und Vollständigkeit sind jedoch uneinheitlich.
- □ Etabliert: Projektauftrag, Scope & Governance ist methodisch umgesetzt, mit abgestimmten Templates, Freigaben und nachvollziehbaren Entscheidungsgrundlagen.
- □ Geübt: Ergebnisse aus Projektauftrag, Scope & Governance werden in Übungen, Reviews, Audits oder Management-Entscheiden aktiv genutzt und verbessert.
- □ Optimiert: Projektauftrag, Scope & Governance ist in Governance, Risiko-, IT-, Lieferanten- und Krisenprozesse integriert und wird mit Kennzahlen gesteuert.

Beratungsfokus

Workshops, Interviews und Vorlagen werden so geführt, dass Entscheidungen, Annahmen, Lücken und Abhängigkeiten sofort sichtbar werden. Der Fokus liegt auf der Umsetzung.

Management-Entscheid

Am Ende des Arbeitsschritts ist klar, welche Freigaben, Ressourcen, Investitionen oder Restrisiken durch Geschäftsleitung / Programmsteuerung entschieden werden müssen.

Nachweis & Pflege

Jedes Ergebnis erhält Eigentümer, Version, Ablageort, Review-Termin und Verbindung zur Massnahmenliste. Dadurch bleibt die Dokumentation auditfähig und praktisch nutzbar.

BCM Policy, Organisation & Methodik

Die BCM Policy übersetzt den Managementauftrag in verbindliche Anforderungen. Sie definiert Zweck, Geltungsbereich, Rollen, Verantwortlichkeiten, Mindeststandards, Review-Zyklus, Übungsanforderungen und die Verbindung zu ISO-22301-orientierten Managementsystem-Elementen.

Policy	Rollen	Methodik	Templates	Freigabe

Policy-Inhalte

Die Policy beschreibt, welche Ziele das BCM verfolgt, wer zuständig ist, welche Prozesse mindestens analysiert werden, wie RTO/RPO, Kritikalität und Risiken bewertet werden und wie Pläne, Schulungen, Tests, Reviews und Verbesserungen gesteuert werden.

Organisationsmodell

Typisch sind Rollen wie Sponsor, BCM-Verantwortliche, Prozessverantwortliche, ITSCM-Verantwortliche, Krisenstabsleitung, Kommunikation, HR, Facility, Einkauf, Legal/Compliance und interne Revision. Wichtig sind Stellvertretungen, Eskalationsrechte und klare Übergänge zum Krisenmanagement.

Methodik und Templates

Ein einheitliches Vorgehen reduziert Aufwand und erhöht Vergleichbarkeit. Festgelegt werden Bewertungsskalen, Zeitfenster für Impact-Bewertung, Kritikalitätsklassen, RTO/RPO-Definition, Risiko-Kategorien, Dokumentenstruktur, Freigaben und Pflegeverantwortung.

Ergebnisse / Deliverables

- BCM Policy
- BCM Rollen- und Verantwortlichkeitsmodell
- BIA-/SIA-/Risiko-Methodik
- Template-Set für Workshops, Interviews und Pläne

Arbeits- und Qualitätscheckliste

Prüfpunkte

- □ Policy ist von der Geschäftsleitung verabschiedet.
- □ Rollen und Stellvertretungen sind dokumentiert und kommuniziert.
- □ Bewertungsskalen und Begriffe werden einheitlich verwendet.
- □ Methodik ist schlank genug für Fachbereiche und präzise genug für Audits.
- □ Pflege, Review und Freigaben sind geregelt.

Reifegrad-Checkliste je Arbeitsschritt

- □ Initial: BCM Policy, Organisation & Methodik ist erkannt, aber Verantwortung, Methode und Nachweise sind noch nicht verlässlich etabliert.
- □ Basis: Vorgehen, Rollen und erste Inhalte zu BCM Policy, Organisation & Methodik sind dokumentiert; Qualität und Vollständigkeit sind jedoch uneinheitlich.
- □ Etabliert: BCM Policy, Organisation & Methodik ist methodisch umgesetzt, mit abgestimmten Templates, Freigaben und nachvollziehbaren Entscheidungsgrundlagen.
- □ Geübt: Ergebnisse aus BCM Policy, Organisation & Methodik werden in Übungen, Reviews, Audits oder Management-Entscheiden aktiv genutzt und verbessert.
- □ Optimiert: BCM Policy, Organisation & Methodik ist in Governance, Risiko-, IT-, Lieferanten- und Krisenprozesse integriert und wird mit Kennzahlen gesteuert.

Beratungsfokus

Der Managementauftrag wird in eine belastbare BCM Policy, ein klares Rollenmodell und eine praxistaugliche Methodik übersetzt. Im Fokus stehen einheitliche Begriffe, Bewertungsskalen, RTO/RPO-Definitionen, Templates, Freigabewege und ein Review-Zyklus, der zu Organisation, Audit und ISO-22301-Orientierung passt.

Management-Entscheid

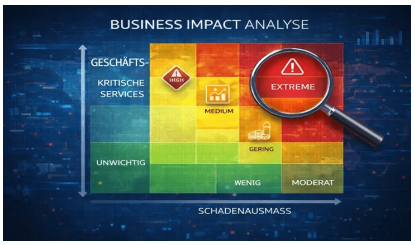
Die Geschäftsleitung verabschiedet Policy, Geltungsbereich, Rollenmodell, Stellvertretungen, Mindestanforderungen, Bewertungsmethodik sowie verbindliche Vorgaben für Reviews, Übungen und Pflege. Damit wird entschieden, wie BCM künftig organisationsweit geführt, angewendet und überprüft wird.

Nachweis & Pflege

Nachweisfähig sind die freigegebene BCM Policy, RACI/Rollenmodell, Methodikbeschreibung, Template-Set und Review-Kalender. Änderungen an Organisation, Prozessen, IT-Services oder regulatorischen Anforderungen werden über definierte Eigentümer, Versionierung und periodische Policy-Reviews gepflegt.

Business Impact Analyse (BIA)

Die BIA ist das Fundament der Priorisierung. Sie identifiziert kritische Geschäftsprozesse, bewertet Auswirkungen über Zeit und leitet Wiederanlaufanforderungen ab. Sie beantwortet, welche Leistungen zuerst wieder funktionieren müssen, welche Ressourcen erforderlich sind und welche Ausfallfolgen tragbar oder nicht tragbar sind.



Scope	Interviews	Impact	RTO/RPO	Priorität	Bericht

Analyseumfang

Die BIA beginnt mit einer Prozess- und Service-Landkarte. Je Prozess werden Eigentümer, Leistungen, Kunden, regulatorische Verpflichtungen, Abhängigkeiten, Ressourcen, Standorte, Schlüsselpersonen, IT-Services, Daten, Dokumente, Lieferanten und Arbeitsmittel erhoben.

Impact-Bewertung

Auswirkungen werden über definierte Zeitfenster beurteilt, zum Beispiel nach Stunden, einem Tag, mehreren Tagen oder Wochen. Bewertet werden finanzielle, operative, rechtliche, regulatorische, reputationsbezogene, kundenbezogene und sicherheitsrelevante Folgen.

RTO, RPO und Priorisierung

Aus der Bewertung entstehen maximale tolerierbare Ausfallzeiten, Recovery Time Objectives, Recovery Point Objectives, Mindestressourcen und Wiederanlaufprioritäten. Die Ergebnisse bilden die Grundlage für BCM-Strategie, BCP, ITSCM, DRP und Management-Entscheide.

Ergebnisse / Deliverables

- BIA-Interviewleitfaden
- Prozess- und Ressourceninventar
- Impact-Matrix je Zeitfenster
- RTO/RPO- und MTPD-Ableitung
- BIA-Bericht mit Wiederanlaufprioritäten

Arbeits- und Qualitätscheckliste

Prüfpunkte

- □ Kritische Prozesse sind vollständig und nachvollziehbar erfasst.
- □ Auswirkungen werden mit einheitlichen Kriterien bewertet.
- □ RTO/RPO wurden fachlich begründet und mit IT abgestimmt.
- □ Abhängigkeiten und Mindestressourcen sind dokumentiert.
- □ Management hat Kritikalität und Prioritäten bestätigt.

Reifegrad-Checkliste je Arbeitsschritt

- □ Initial: Business Impact Analyse (BIA) ist erkannt, aber Verantwortung, Methode und Nachweise sind noch nicht verlässlich etabliert.
- □ Basis: Vorgehen, Rollen und erste Inhalte zu Business Impact Analyse (BIA) sind dokumentiert; Qualität und Vollständigkeit sind jedoch uneinheitlich.
- □ Etabliert: Business Impact Analyse (BIA) ist methodisch umgesetzt, mit abgestimmten Templates, Freigaben und nachvollziehbaren Entscheidungsgrundlagen.
- □ Geübt: Ergebnisse aus Business Impact Analyse (BIA) werden in Übungen, Reviews, Audits oder Management-Entscheiden aktiv genutzt und verbessert.
- □ Optimiert: Business Impact Analyse (BIA) ist in Governance, Risiko-, IT-, Lieferanten- und Krisenprozesse integriert und wird mit Kennzahlen gesteuert.

Beratungsfokus

Wir strukturieren BIA-Interviews mit Prozessverantwortlichen, erfassen Leistungen, Abhängigkeiten, Ressourcen, IT-Services, Lieferanten und Ausfallfolgen über definierte Zeitfenster. Ziel ist eine nachvollziehbare Herleitung von Kritikalität, MTPD, RTO, RPO, Mindestressourcen und Wiederanlaufprioritäten.

Management-Entscheid

Das Management bestätigt, welche Prozesse kritisch sind, welche Ausfallzeiten tragbar bleiben, welche Wiederanlaufprioritäten gelten und welche Ressourcen zwingend verfügbar sein müssen. Konflikte zwischen Business-Anforderungen, IT-Fähigkeiten und verfügbaren Mitteln werden transparent entschieden.

Nachweis & Pflege

Die BIA-Ergebnisse werden als validierter BIA-Bericht, Prozess- und Ressourceninventar, Impact-Matrix sowie RTO/RPO-Übersicht geführt. Aktualisierungen erfolgen bei Prozessänderungen, neuen Services, veränderten Kundenanforderungen, Lieferantenwechseln oder nach Übungen und Ereignissen.

Risikoanalyse & Lagebild Ausfallkritikalität

Die Risikoanalyse ergänzt die BIA. Während die BIA zeigt, was kritisch ist, zeigt die Risikoanalyse, wodurch kritische Leistungen ausfallen können. Das Lagebild verbindet Prozesskritikalität, Serviceabhängigkeiten, Bedrohungen, Schwachstellen und bestehende Massnahmen zu einer priorisierten Sicht.

Szenarien	Schwachstellen	Kontrollen	Restrisiko	Massnahmen

Szenarien

Typische Szenarien sind Cyberangriff, Ransomware, IT-Ausfall, Stromunterbruch, Gebäudeausfall, Brand, Wasser, Pandemie, Personalausfall, Lieferantenausfall, Transportstörung, Reputationskrise, regulatorische Eskalation oder Ausfall eines kritischen Dienstleisters.

Bewertung

Bewertet werden Eintrittsnähe, Verwundbarkeit, Auswirkung auf kritische Prozesse, bestehende Kontrollen, Detektionsfähigkeit, Wiederherstellbarkeit und Restexposition. Wichtig ist, nicht nur technische Einzelrisiken, sondern die Wirkung auf geschäftskritische Leistungen zu betrachten.

Lagebild und Massnahmen

Das Lagebild priorisiert Massnahmen: präventive Reduktion, vorbereitete Ersatzverfahren, Recovery-Kapazitäten, Krisenkommunikation, Supplier-Alternativen, IT-Resilienz und organisatorische Übungen. Ergebnis ist eine klare Entscheidgrundlage für Strategie und Investition.

Ergebnisse / Deliverables

- Szenario- und Risiko-Katalog
- Lagebild Service-Ausfallkritikalität
- Risikomatrix mit Kritikalitätsbezug
- Entscheidvorlage für Restrisiko und Prioritäten
- Massnahmenportfolio und Quick Wins

Arbeits- und Qualitätscheckliste

Prüfpunkte

- □ Risikoszenarien decken Business, IT, Gebäude, Personal und Lieferanten ab.
- □ Bewertung ist mit BIA-Kritikalität verknüpft.
- □ Bestehende Kontrollen und Lücken sind sichtbar.
- □ Massnahmen sind priorisiert, budgetierbar und verantwortet.
- □ Lagebild wird regelmässig aktualisiert.

Reifegrad-Checkliste je Arbeitsschritt

- □ Initial: Risikoanalyse & Lagebild Ausfallkritikalität ist erkannt, aber Verantwortung, Methode und Nachweise sind noch nicht verlässlich etabliert.
- □ Basis: Vorgehen, Rollen und erste Inhalte zu Risikoanalyse & Lagebild Ausfallkritikalität sind dokumentiert; Qualität und Vollständigkeit sind jedoch uneinheitlich.
- □ Etabliert: Risikoanalyse & Lagebild Ausfallkritikalität ist methodisch umgesetzt, mit abgestimmten Templates, Freigaben und nachvollziehbaren Entscheidungsgrundlagen.
- □ Geübt: Ergebnisse aus Risikoanalyse & Lagebild Ausfallkritikalität werden in Übungen, Reviews, Audits oder Management-Entscheiden aktiv genutzt und verbessert.
- □ Optimiert: Risikoanalyse & Lagebild Ausfallkritikalität ist in Governance, Risiko-, IT-, Lieferanten- und Krisenprozesse integriert und wird mit Kennzahlen gesteuert.

Beratungsfokus

Wir verbinden Risikoszenarien mit der BIA-Kritikalität und zeigen, wodurch kritische Leistungen tatsächlich ausfallen können. Betrachtet werden Cyberangriffe, IT-Ausfälle, Gebäudeereignisse, Personalengpässe, Lieferantenausfälle, regulatorische Eskalationen sowie bestehende Kontrollen und Schwachstellen.

Management-Entscheid

Die Geschäftsleitung entscheidet, welche Restrisiken akzeptiert werden, welche Massnahmen priorisiert werden und wo Investitionen in Prävention, Notbetrieb, Recovery-Fähigkeit, Lieferantenalternativen oder organisatorische Vorbereitung erforderlich sind. Das Lagebild wird zur Grundlage für Strategie und Budget.

Nachweis & Pflege

Nachweisfähig sind Szenariokatalog, Risikomatrix, Lagebild, Kontrollbewertung, Restrisikobewertung und Massnahmenportfolio. Das Lagebild wird nach Incidents, Audits, Übungen, wesentlichen IT- oder Lieferantenänderungen sowie periodisch im Risikomanagement aktualisiert.

Business Continuity Strategie

Die BCM-Strategie ist die Brücke zwischen Analyse und Umsetzung. Sie definiert, wie kritische Prozesse bei Störungen fortgeführt oder innerhalb definierter Wiederanlaufzeiten wiederhergestellt werden. Sie ist ein Management-Entscheid über Zielniveau, Ressourcen, Restrisiko und Wirtschaftlichkeit.

Anforderung	Option	Bewertung	Entscheid	Planung

Strategieoptionen

Optionen sind Ersatzarbeitsplätze, Homeoffice, Schichtbetrieb, manuelle Ersatzprozesse, priorisierte Kundenbedienung, alternative Lieferanten, Sicherheitsbestände, Outsourcing, Redundanz, Cloud-/Backup-Lösungen, Notfallkommunikation, Verlagerung von Aufgaben oder temporäre Leistungsreduktion.

Bewertung und Entscheidung

Jede Option wird hinsichtlich Wirksamkeit, Machbarkeit, Kosten, Umsetzungszeit, Risiken, Abhängigkeiten und regulatorischer Anforderungen bewertet. Die Geschäftsleitung entscheidet, welche Wiederanlaufziele verbindlich sind und welche Restrisiken akzeptiert werden.

Umsetzungsvorbereitung

Die Strategie muss in konkrete Pläne übersetzbar sein. Deshalb werden Verantwortliche, Ressourcen, Voraussetzungen, Auslösekriterien, Eskalationslogik, Kommunikationsbedarf und Testbarkeit festgelegt. Nicht umsetzbare Strategien werden verworfen oder als langfristige Massnahmen markiert.

Ergebnisse / Deliverables

- BCM-Strategiepapier
- Optionsbewertung mit Kosten/Nutzen/Risiko
- Management-Entscheid zu Restrisiko und Zielniveau
- Massnahmenplan zur Strategieumsetzung
- Vorgaben für BCP, DRP, SCP und VCP

Arbeits- und Qualitätscheckliste

Prüfpunkte

- □ Strategie basiert auf BIA, Risikoanalyse und Ressourcenrealität.
- □ Optionen sind fachlich und wirtschaftlich bewertet.
- □ Management hat Prioritäten und Restrisiko entschieden.
- □ Strategien sind in Pläne, Verträge oder technische Massnahmen überführbar.
- □ Testbarkeit und Pflege sind berücksichtigt.

Reifegrad-Checkliste je Arbeitsschritt

- □ Initial: Business Continuity Strategie ist erkannt, aber Verantwortung, Methode und Nachweise sind noch nicht verlässlich etabliert.
- □ Basis: Vorgehen, Rollen und erste Inhalte zu Business Continuity Strategie sind dokumentiert; Qualität und Vollständigkeit sind jedoch uneinheitlich.
- □ Etabliert: Business Continuity Strategie ist methodisch umgesetzt, mit abgestimmten Templates, Freigaben und nachvollziehbaren Entscheidungsgrundlagen.
- □ Geübt: Ergebnisse aus Business Continuity Strategie werden in Übungen, Reviews, Audits oder Management-Entscheiden aktiv genutzt und verbessert.
- □ Optimiert: Business Continuity Strategie ist in Governance, Risiko-, IT-, Lieferanten- und Krisenprozesse integriert und wird mit Kennzahlen gesteuert.

Beratungsfokus

Wir entwickeln aus BIA und Risikoanalyse konkrete Continuity-Optionen wie Notbetrieb, Ersatzarbeitsplätze, Homeoffice, manuelle Ersatzprozesse, alternative Lieferanten, Sicherheitsbestände, Redundanz, Backup- oder Recovery-Lösungen. Jede Option wird auf Wirksamkeit, Machbarkeit, Kosten, Abhängigkeiten und Testbarkeit geprüft.

Management-Entscheid

Das Management entscheidet Zielniveau, verbindliche Wiederanlaufziele, Strategieoptionen je kritischem Prozess, Investitionsbedarf, Umsetzungsreihenfolge und akzeptierte Restrisiken. Nicht realistische oder wirtschaftlich nicht vertretbare Optionen werden bewusst verworfen oder als langfristige Massnahmen geführt.

Nachweis & Pflege

Dokumentiert werden Strategiepapier, Optionsbewertung, Kosten-/Nutzen-/Risikovergleich, Managemententscheid, Massnahmenplan und Vorgaben für BCP, DRP, SCP und VCP. Die Strategie wird bei neuen BIA-Ergebnissen, veränderten Risiken, Tests oder Geschäftsänderungen überprüft.

Business Continuity Plan (BCP)

Business Continuity Pläne machen die Strategie handlungsfähig. Sie enthalten klare Rollen, Auslösekriterien, Sofortmassnahmen, Notbetrieb, Wiederanlauf, Kommunikation, Kontaktlisten, Schnittstellen und Checklisten. Ein guter BCP ist verständlich, kurz genug für den Ereignisfall und präzise genug für die Umsetzung.

Auslöser	Sofortmassnahmen	Notbetrieb	Wiederanlauf	Review

Planstruktur

Ein BCP enthält Zweck, Scope, Auslöser, Alarmierung, Rollen, Verantwortlichkeiten, Stellvertretungen, Lageerfassung, Entscheidpunkte, Kommunikationswege, Sofortmassnahmen, Notbetriebsverfahren, Wiederanlaufverfahren, Ressourcen, Kontaktlisten, Anhänge und Pflegeinformationen.

Praxistauglichkeit

Der Plan muss unter Stress funktionieren. Dazu braucht es klare Sprache, priorisierte Schritte, Checklisten, Telefonnummern, alternative Kommunikationswege, Versionierung, Offline-Verfügbarkeit und eindeutige Zuständigkeiten. Fachbereiche müssen den Plan selbst anwenden können.

Integration

BCP sind mit Krisenmanagement, ITSCM/DRP, HR, Kommunikation, Facility, Einkauf, Legal/Compliance und Lieferantenplänen abgestimmt. Kritische Schnittstellen, Übergaben und Eskalationen müssen beschrieben sein, sonst entstehen im Ereignisfall Lücken.

Ergebnisse / Deliverables

- BCP-Template und Schreibanleitung
- Business Continuity Plan je kritischem Prozess
- Kontakt-, Ressourcen- und Stellvertreterlisten
- Checklisten für Sofortmassnahmen und Notbetrieb
- Freigabe-, Ablage- und Pflegekonzept

Arbeits- und Qualitätscheckliste

Prüfpunkte

- □ BCP sind an den kritischen Prozessen ausgerichtet.
- □ Auslöser, Eskalation und Rollen sind eindeutig beschrieben.
- □ Notbetrieb und Wiederanlauf sind schrittweise umsetzbar.
- □ Kontaktlisten und Ressourcen sind aktuell.
- □ Pläne wurden mit Beteiligten geprüft und getestet.

Reifegrad-Checkliste je Arbeitsschritt

- □ Initial: Business Continuity Pläne (BCP) ist erkannt, aber Verantwortung, Methode und Nachweise sind noch nicht verlässlich etabliert.
- □ Basis: Vorgehen, Rollen und erste Inhalte zu Business Continuity Pläne (BCP) sind dokumentiert; Qualität und Vollständigkeit sind jedoch uneinheitlich.
- □ Etabliert: Business Continuity Pläne (BCP) ist methodisch umgesetzt, mit abgestimmten Templates, Freigaben und nachvollziehbaren Entscheidungsgrundlagen.
- □ Geübt: Ergebnisse aus Business Continuity Pläne (BCP) werden in Übungen, Reviews, Audits oder Management-Entscheiden aktiv genutzt und verbessert.
- □ Optimiert: Business Continuity Pläne (BCP) ist in Governance, Risiko-, IT-, Lieferanten- und Krisenprozesse integriert und wird mit Kennzahlen gesteuert.

Beratungsfokus

Wir überführen die BCM-Strategie in anwendbare Business Continuity Pläne mit Auslösekriterien, Alarmierung, Rollen, Sofortmassnahmen, Notbetrieb, Wiederanlauf, Kommunikation, Kontaktlisten und Schnittstellen. Der Fokus liegt auf kurzen, klaren und unter Stress nutzbaren Handlungsanweisungen.

Management-Entscheid

Freigegeben werden BCP-Struktur, Auslöser, Eskalationsrechte, Notbetriebsniveau, Wiederanlaufreihenfolge, verantwortliche Rollen, benötigte Ressourcen, Offline-Verfügbarkeit und Testplan. Damit entscheidet die Organisation, wie kritische Prozesse im Ereignisfall praktisch weitergeführt werden.

Nachweis & Pflege

Nachweisfähig sind freigegebene BCP, Kontakt- und Stellvertreterlisten, Ressourcenübersichten, Testprotokolle und Review-Nachweise. Pflege erfolgt nach Personal-, Standort-, Prozess-, IT- oder Lieferantenänderungen sowie nach Walkthroughs, Übungen und realen Ereignissen.

ITSCM, Service Impact Analyse (SIA) & Disaster Recovery (DRP)

IT Service Continuity Management stellt sicher, dass IT-Services die Wiederanlaufziele des Business unterstützen. Die Service Impact Analyse priorisiert IT-Services nach Geschäftsauswirkung. Der Disaster Recovery Plan beschreibt die technische Wiederherstellung von Systemen, Daten, Infrastruktur, Schnittstellen und Arbeitsfähigkeit.

Service Impact Analyse (SIA)	Mapping IT-Service / Infrastruktur	RTO/RPO	Recovery	Disaster Recovery Plan (DRP)	Test

SIA und Service Mapping

Die SIA verbindet Geschäftsprozesse mit IT-Services, Applikationen, Datenbanken, Schnittstellen, Infrastruktur, Cloud-Diensten, Netzwerken, Identitäten, Dienstleistern und Betriebsprozessen. Dadurch wird sichtbar, welche technischen Komponenten für welche Geschäftsleistungen kritisch sind.

Recovery-Strategie

Für kritische Services werden RTO, RPO, Backup, Restore, Redundanz, Failover, Ersatzinfrastruktur, Cyber-Recovery, manuelle Übergangslösungen und Abhängigkeiten bewertet. Ziel ist eine realistische technische Strategie, die Business-Anforderungen erfüllt.

DRP und Test

Der DRP enthält Schritt-für-Schritt-Verfahren, Verantwortlichkeiten, Prioritäten, technische Voraussetzungen, Kommunikationswege, Entscheidpunkte, Abbruchkriterien und Testnachweise. Ohne regelmässige Tests bleibt Recovery eine Annahme, kein Nachweis.

Ergebnisse / Deliverables

- IT-Service-Katalog und Kritikalitätsbewertung
- Service-to-Process-Mapping
- RTO/RPO-Abgleich zwischen Business und IT
- Disaster Recovery Plan und Runbooks
- DRP-Testkonzept, Protokoll und Massnahmenliste

Arbeits- und Qualitätscheckliste

Prüfpunkte

- □ Kritische IT-Services sind mit Geschäftsprozessen verknüpft.
- □ RTO/RPO sind zwischen Business und IT abgestimmt.
- □ Backup-/Restore- und Failover-Verfahren sind dokumentiert.
- □ Technische Abhängigkeiten und Dienstleister sind berücksichtigt.
- □ DRP wurde realitätsnah getestet.

Reifegrad-Checkliste je Arbeitsschritt

- □ Initial: ITSCM, SIA & Disaster Recovery ist erkannt, aber Verantwortung, Methode und Nachweise sind noch nicht verlässlich etabliert.
- □ Basis: Vorgehen, Rollen und erste Inhalte zu ITSCM, SIA & Disaster Recovery sind dokumentiert; Qualität und Vollständigkeit sind jedoch uneinheitlich.
- □ Etabliert: ITSCM, SIA & Disaster Recovery ist methodisch umgesetzt, mit abgestimmten Templates, Freigaben und nachvollziehbaren Entscheidungsgrundlagen.
- □ Geübt: Ergebnisse aus ITSCM, SIA & Disaster Recovery werden in Übungen, Reviews, Audits oder Management-Entscheiden aktiv genutzt und verbessert.
- □ Optimiert: ITSCM, SIA & Disaster Recovery ist in Governance, Risiko-, IT-, Lieferanten- und Krisenprozesse integriert und wird mit Kennzahlen gesteuert.

Beratungsfokus

Wir verknüpfen Geschäftsprozesse mit IT-Services, Applikationen, Datenbanken, Infrastruktur, Cloud-Diensten, Identitäten, Schnittstellen und Providern. Daraus entstehen Service Impact Analyse, RTO/RPO-Abgleich, realistische Recovery-Strategien, DRP-Runbooks und testbare technische Wiederherstellungsverfahren.

Management-Entscheid

Entschieden werden Recovery-Prioritäten, technische Zielwerte, Backup-/Restore- und Failover-Fähigkeiten, Cyber-Recovery-Anforderungen, Investitionen in Redundanz oder Ersatzinfrastruktur sowie akzeptierte Lücken zwischen Business-Anforderung und technischer Wiederherstellbarkeit.

Nachweis & Pflege

Nachweisfähig sind Service-to-Process-Mapping, IT-Service-Kritikalität, RTO/RPO-Abgleich, DRP, technische Runbooks, Restore- und Failover-Testprotokolle. Aktualisierung erfolgt bei Releases, Architekturänderungen, Providerwechseln, neuen Cloud-Services, Cyber-Erkenntnissen oder DRP-Tests.

Supplier & Vendor Continuity Management

Externe Abhängigkeiten sind oft kritische Schwachstellen. Supplier Continuity fokussiert auf Lieferketten, Materialien und Dienstleistungen. Vendor Continuity fokussiert auf externe Dienstleister, Outsourcing, kritische Plattformen, IT-Provider und Beschaffungsbeziehungen. Beide Ansätze sichern die Verfügbarkeit externer Leistungen.

Klassieren | **Bewerten** | **Strategie** | **Vertrag** | **Plan** | **Monitoring**

Kritikalität und Risk Rating

Lieferanten und Dienstleister werden nach Einfluss auf kritische Prozesse, Substituierbarkeit, Wiederbeschaffungszeit, Vertragsbindung, geografischem Risiko, Finanzstabilität, Cyber-/IT-Risiko, Compliance, Qualität und Abhängigkeit bewertet.

Kontinuitätsstrategien

Mögliche Strategien sind Zweitlieferanten, Sicherheitsbestände, alternative Logistik, vertragliche BCM-Anforderungen, Nachweispflichten, Eskalationskontakte, Notfall-SLAs, gemeinsame Übungen, Exit-Strategien und Monitoring.

Pläne und Zusammenarbeit

Für kritische Partner entstehen Supplier Continuity Plans oder Vendor Continuity Plans mit Rollen, Auslösern, Kommunikationswegen, Ersatzoptionen, Eskalation, Recovery-Erwartungen und Massnahmen. Entscheidend ist, dass Einkauf, Fachbereich, Legal, Risiko, IT und Lieferant beteiligt sind.

Ergebnisse / Deliverables

- Kritische Lieferanten-/Vendor-Liste
- Supplier/Vendor Risk Rating
- Backup- und Alternativstrategien
- SCP/VCP-Templates und Pläne
- Monitoring-, KPI- und Review-Konzept

Arbeits- und Qualitätscheckliste

Prüfpunkte

- □ Kritische externe Abhängigkeiten sind vollständig identifiziert.
- □ Risk Rating berücksichtigt Business-, Finanz-, Cyber-, Geo- und Compliance-Aspekte.
- □ Alternativen und Eskalationen sind realistisch verfügbar.
- □ Verträge und SLAs enthalten Continuity-Anforderungen.
- □ Lieferanten-/Vendor-Pläne werden überprüft und aktualisiert.

Reifegrad-Checkliste je Arbeitsschritt

- □ Initial: Supplier & Vendor Continuity ist erkannt, aber Verantwortung, Methode und Nachweise sind noch nicht verlässlich etabliert.
- □ Basis: Vorgehen, Rollen und erste Inhalte zu Supplier & Vendor Continuity sind dokumentiert; Qualität und Vollständigkeit sind jedoch uneinheitlich.
- □ Etabliert: Supplier & Vendor Continuity ist methodisch umgesetzt, mit abgestimmten Templates, Freigaben und nachvollziehbaren Entscheidungsgrundlagen.
- □ Geübt: Ergebnisse aus Supplier & Vendor Continuity werden in Übungen, Reviews, Audits oder Management-Entscheiden aktiv genutzt und verbessert.
- □ Optimiert: Supplier & Vendor Continuity ist in Governance, Risiko-, IT-, Lieferanten- und Krisenprozesse integriert und wird mit Kennzahlen gesteuert.

Beratungsfokus

Wir identifizieren kritische Lieferanten und Dienstleister, bewerten Substituierbarkeit, Wiederbeschaffungszeit, Vertragsbindung, geografische Risiken, Finanzstabilität, Cyber-/IT-Risiken und Compliance. Daraus entstehen Risk Rating, Backup-Strategien, Eskalationswege, Vertragsanforderungen und Continuity-Pläne.

Management-Entscheid

Das Management bestätigt kritische Supplier/Vendor, akzeptierte Single-Source-Risiken, notwendige Alternativstrategien, vertragliche BCM-Anforderungen, Notfall-SLAs, Eskalationskontakte und Monitoring-Kennzahlen. Kritische Abhängigkeiten werden damit bewusst gesteuert statt nur dokumentiert.

Nachweis & Pflege

Nachweisfähig sind kritische Lieferantenliste, Risk Rating, Continuity-Nachweise, Vertragsklauseln, SCP/VCP-Pläne, Eskalationskontakte und Monitoring-Berichte. Pflege erfolgt im Beschaffungsprozess, bei Vertragsänderungen, Lieferantenwechseln, Incidents, Audits und periodischen Reviews.

Krisenmanagement, Schulung, Übung & Review

Continuity wird erst belastbar, wenn Menschen, Rollen, Entscheidwege, Kommunikation und Wiederanlaufverfahren trainiert sind. Krisenmanagement sorgt für Führung unter erschwerten Bedingungen; Übungen zeigen, ob BCP, DRP, Supplier/Vendor-Pläne und Krisenorganisation wirklich funktionieren.

Alarmieren | Führen | Entscheiden | Kommunizieren | Wiederanlauf | Verbessern

Krisenorganisation

Definiert werden Alarmierung, Krisenstab, Rollen, Lagebild, Entscheidungsrhythmus, Protokoll, Auftragscontrolling, interne und externe Kommunikation, Medienarbeit, Stakeholder-Management, Schnittstellen zu IT, HR, Legal, Facility, Einkauf und Geschäftsleitung.

Übungsdesign

Übungen reichen von Dokumentenreview über Walkthrough, Tabletop-Übung, technischem DRP-Test, Krisenstabsübung bis zu integrierten Szenarien mit Business, IT, Lieferanten und Kommunikation. Ein gutes Drehbuch erzeugt realistische Entscheidungen und messbare Erkenntnisse.

Review und Verbesserung

Nach jeder Übung werden Beobachtungen, Abweichungen, Entscheidungen, Kommunikationslücken, technische Probleme und Planverbesserungen dokumentiert. Massnahmen erhalten Verantwortliche, Fristen und Management-Nachverfolgung.

Ergebnisse / Deliverables

- Krisenmanagement- und Übungskonzept
- Übungsdrehbuch mit Injects
- Teilnehmer-, Beobachter- und Bewertungsbogen
- Lessons-Learned-Bericht
- Massnahmenplan mit Verantwortlichkeiten und Fristen

Arbeits- und Qualitätscheckliste

Prüfpunkte

- □ Krisenrollen sind besetzt, geschult und stellvertreten.
- □ Alarmierung, Lagebild und Kommunikationswege sind getestet.
- □ Übungsszenarien prüfen reale Entscheid- und Wiederanlaufanforderungen.
- □ Lessons Learned führen zu konkreten Plan- und Prozessverbesserungen.
- □ Management verfolgt Massnahmen bis zur Umsetzung.

Reifegrad-Checkliste je Arbeitsschritt

- □ Initial: Krisenmanagement, Schulung, Übung & Review ist erkannt, aber Verantwortung, Methode und Nachweise sind noch nicht verlässlich etabliert.
- □ Basis: Vorgehen, Rollen und erste Inhalte zu Krisenmanagement, Schulung, Übung & Review sind dokumentiert; Qualität und Vollständigkeit sind jedoch uneinheitlich.
- □ Etabliert: Krisenmanagement, Schulung, Übung & Review ist methodisch umgesetzt, mit abgestimmten Templates, Freigaben und nachvollziehbaren Entscheidungsgrundlagen.
- □ Geübt: Ergebnisse aus Krisenmanagement, Schulung, Übung & Review werden in Übungen, Reviews, Audits oder Management-Entscheiden aktiv genutzt und verbessert.
- □ Optimiert: Krisenmanagement, Schulung, Übung & Review ist in Governance, Risiko-, IT-, Lieferanten- und Krisenprozesse integriert und wird mit Kennzahlen gesteuert.

Beratungsfokus

Wir verbinden Krisenorganisation, Alarmierung, Lagebild, Entscheidungsrhythmus, Kommunikation und Wiederanlauf mit BCP, DRP sowie Supplier/Vendor-Plänen. Übungen werden mit realistischen Szenarien, Injects, Beobachtungskriterien und klaren Lernzielen vorbereitet und ausgewertet.

Management-Entscheid

Freigegeben werden Krisenrollen, Stellvertretungen, Alarmierungswege, Übungsziele, Szenarioumfang, Kommunikationsfreigaben, Beobachtungskriterien und Ressourcen für Verbesserungsmassnahmen. Das Management entscheidet, welche Fähigkeiten trainiert und welche Lücken prioritär geschlossen werden.

Nachweis & Pflege

Nachweisfähig sind Schulungsunterlagen, Teilnehmerlisten, Übungsdrehbuch, Beobachtungsbogen, Lessons-Learned-Bericht und Massnahmen-Tracking. Pflege erfolgt über aktualisierte Pläne, geschlossene Massnahmen, erneute Tests und Management-Reviews bis zur nachweisbaren Wirksamkeit.

Projektpakete & Deliverables

Die Projektpakete können einzeln, kombiniert oder als Gesamtprogramm umgesetzt werden. Jedes Paket hat einen klaren Zweck, typische Aktivitäten und konkrete Deliverables. Dadurch kann die Organisation klein starten, priorisiert ausbauen und gleichzeitig die Management- und Auditfähigkeit sicherstellen.

Paket 1 - Quick Assessment und Management-Roadmap

Kurzanalyse bestehender Dokumente, Interviews mit Schlüsselpersonen, Reifegradbewertung, Gap-Analyse, Risikolagebild und priorisierte Roadmap. Deliverables: Assessment-Bericht, Heatmap, Quick-Win-Liste, Management-Präsentation, Umsetzungsplan mit Aufwand, Priorität und Verantwortlichkeit.

Paket 2 - BCMS, Governance und Policy

Aufbau des BCM-Rahmenwerks mit Policy, Rollenmodell, Methodenbeschreibung, Template-Set, Review-Kalender und Berichtswesen. Deliverables: BCM Policy, RACI, Governance-Board, Methodikhandbuch, BIA-/Risiko-/BCP-Templates, Kommunikationsunterlagen.

Paket 3 - BIA, Risikoanalyse und Strategie

Workshops mit Fachbereichen, Impact-Bewertung, RTO/RPO, Abhängigkeitsanalyse, Risikoanalyse, Strategieoptionen und Management-Entscheid. Deliverables: BIA-Bericht, Kritikalitätsmatrix, Ressourceninventar, Risikomatrix, BCM-Strategiepapier, Entscheidvorlage.

Paket 4 - BCP, ITSCM und DRP

Erstellung praxistauglicher Pläne für kritische Prozesse und IT-Services. Deliverables: BCP je Prozess, IT-Service-Kritikalitätslagebild, Service Mapping, DRP, Recovery-Runbooks, Kontaktlisten, Notbetriebschecklisten, Ablage- und Pflegekonzept.

Paket 5 - Supplier/Vendor Continuity

Kritikalität externer Partner, Risk Rating, Kontinuitätsanforderungen, Backup-Strategien und Eskalationspläne. Deliverables: kritische Supplier-/Vendor-Liste, Risk-Rating-Modell, SCP/VCP-Pläne, Vertragsklauseln, Monitoring-Konzept.

Paket 6 - Schulung, Übungen und Nachweis

Trainings, Tabletop-Übungen, Krisenstabsübungen, DRP-Tests und Auswertung. Deliverables: Schulungsunterlagen, Übungsdrehbuch, Beobachtungsbogen, Lessons-Learned-Bericht, Massnahmen-Tracking, Management-Review.

Paket 7 - ISO-22301-Coaching und Auditfähigkeit

Gap-Analyse, Normabgleich, Dokumentationsprüfung, Wirksamkeitsnachweise und Auditvorbereitung. Deliverables: ISO-22301-Gap-Bericht, Nachweismatrix, Audit-Agenda, Korrekturmassnahmenplan, Management-Review-Unterlagen.

Projektpakete / Deliverables / Nachweise

- Assessment-Bericht
- BCM Policy
- BIA-/SIA-Bericht
- BCM-Strategie
- BCP/DRP/SCP/VCP
- Übungsbericht
- ISO-22301-Nachweismatrix

Management-Nutzen

Wir strukturieren das Projekt in klare Leistungspakete mit definierten Aktivitäten, Ergebnissen und Nachweisen. Die Bausteine werden so kombiniert, dass Aufwand, Nutzen, Reifegrad und Auditfähigkeit optimal zusammenpassen.

Beratungsansatz

Das Management priorisiert die Projektpakete und legt Scope, Reihenfolge, Budget, Ressourcen, Zielreifegrad und Deliverables fest. So wird klar, ob Standortbestimmung, BCM-Rahmenwerk, operative Pläne, Lieferantenresilienz, Übungsnachweise oder ISO-22301-Auditfähigkeit zuerst umgesetzt werden.

Ergebnisqualität

Nachweisfähig sind Paketauftrag, Deliverable-Matrix, Abnahmen, Assessment-Bericht, Policy, BIA-/SIA-Berichte, Strategie, BCP/DRP/SCP/VCP, Übungsberichte und ISO-22301-Nachweismatrix. Jedes Paket erhält Eigentümer, Version, Ablageort, Review-Termin und offene Massnahmen.

180-Tage-Umsetzungsplan

Ein fokussierter 180-Tage-Plan schafft Momentum und zeigt der Geschäftsleitung früh belastbare Ergebnisse. Der Plan eignet sich für Organisationen, die BCM neu aufbauen, bestehende Unterlagen aktualisieren oder ein Audit-/Kunden-/Regulatorik-Erfordernis strukturiert beantworten müssen.

Tag 1-30 Kick-off	Tag 31-70 BIA	Tag 71-100 Risiko	Tag 101-130 Strategie	Tag 131-160 Pläne	Tag 161-180 Review

Tag 1-30: Initiierung

Kick-off, Dokumentenreview, Scope, Stakeholder, Governance, Projektplan, Methodik, Workshopplanung und Kommunikationspaket. Ergebnis: freigegebener Projektauftrag und klare Arbeitslogik.

Tag 31-70: BIA und Kritikalität

Interviews und Workshops mit priorisierten Bereichen. Erhebung kritischer Prozesse, Auswirkungen, Ressourcen, RTO/RPO, Standorte, IT-Services, Lieferanten und Schlüsselpersonen. Ergebnis: erste Kritikalitätsmatrix und Priorisierung.

Tag 71-100: Risiko und Lagebild

Szenarioanalyse, bestehende Massnahmen, Lücken, Quick Wins, Abhängigkeiten, Service-Ausfallkritikalität und Massnahmenportfolio. Ergebnis: verdichtetes Lagebild für Management-Entscheide.

Tag 101-130: BCM-Strategie

Strategieoptionen entwickeln, bewerten und mit Geschäftsleitung entscheiden. Ergebnis: Zielniveau, Restrisiko, Investitionsbedarf und Umsetzungsroadmap.

Tag 131-160: Pilot-Pläne

Pilot-BCP und optional Pilot-DRP/SCP/VCP erstellen, Kontaktlisten und Checklisten definieren, Ablagekonzept und Pflegeverantwortung regeln. Ergebnis: erste nutzbare Continuity-Dokumente.

Tag 161-180: Management-Review

Walkthrough, Lessons Learned, Massnahmen, Plan für nächsten Umsetzungszyklus, Management-Präsentation und Entscheidungsvorlage. Ergebnis: geprüfte Ergebnisse und freigegebene nächste Schritte.

Management-Checkliste

- □ Nach 70 Tagen liegt Transparenz über Scope, Stakeholder und erste Kritikalitäten vor.
- □ Nach 130 Tagen sind Risiken, Lücken und Strategieoptionen entscheidungsfähig.
- □ Nach 160 Tagen existieren Pilot-Pläne, Roadmap und Management-Review.
- □ Die nächsten Umsetzungswellen sind priorisiert und budgetierbar.

Management-Nutzen

Wir verdichten den BCM-Aufbau in einen fokussierten 180-Tage-Zyklus mit Meilensteinen: Kick-off, BIA, Risikoanalyse, Strategieentscheid, Pilot-Pläne und Management-Review. Der Fokus liegt auf schneller Transparenz, sichtbaren Ergebnissen, belastbaren Managemententscheiden und praxistauglichen Continuity-Dokumenten statt auf langwieriger Grundlagendokumentation.

Beratungsansatz

Nach 70 Tagen werden Scope, Stakeholder, Governance und erste Kritikalitäten bestätigt. Nach 130 Tagen entscheidet das Management über Risiken, Lücken, Strategieoptionen, Ressourcen und Restrisiken. Nach 160 Tagen werden Pilot-Pläne, Roadmap, nächste Umsetzungswellen, Budgetbedarf und Verantwortlichkeiten freigegeben.

Ergebnisqualität

Nachweisfähig sind Projektauftrag, Workshop-Protokolle, BIA-Zwischenergebnisse, Kritikalitätsmatrix, Risikolagebild, Strategieentscheid, Pilot-BCP, Pilot-DRP/SCP/VCP, Management-Präsentation und Massnahmenliste. Die Ergebnisse des 90-Tage-Zyklus werden in eine priorisierte Roadmap, Review-Kalender und Massnahmen-Tracking überführt.

Reifegradmodell & Steuerungskennzahlen

Das Reifegradmodell dient als gemeinsames Bewertungsraster für Management, Projektleitung, Fachbereiche und Audit. Es zeigt, ob BCM nur dokumentiert, tatsächlich eingeführt oder bereits geübt und optimiert ist. Ergänzend helfen Kennzahlen, Fortschritt, Wirksamkeit und Pflegequalität zu steuern.

Reifegrad 1 - Initial

Einzelne Dokumente oder Absichten sind vorhanden. Rollen, Scope, Methode, Freigaben und Tests sind noch unklar. Abhängigkeit von Einzelpersonen ist hoch.

Reifegrad 2 - Basis

Grundlegende Policy, erste BIA, erste Pläne oder Risikoübersichten bestehen. Die Anwendung ist jedoch noch nicht vollständig konsistent, gepflegt oder geübt.

Reifegrad 3 - Etabliert

Methodik, Rollen, kritische Prozesse, Strategien, Pläne und Verantwortlichkeiten sind dokumentiert, abgestimmt und freigegeben. Schnittstellen zu IT, Lieferanten und Krisenmanagement sind erkennbar.

Reifegrad 4 - Geübt

Pläne, Alarmierung, Krisenrollen und Recovery-Verfahren werden regelmässig getestet. Lessons Learned führen zu nachvollziehbaren Verbesserungen.

Reifegrad 5 - Optimiert

BCM ist in Governance, Risiko, ITSM, Informationssicherheit, Supplier Management und strategische Planung integriert. Kennzahlen, Audits und Management-Reviews steuern die Weiterentwicklung.

Projektpakete / Deliverables / Nachweise

- KPI: Anteil kritischer Prozesse mit aktueller BIA
- KPI: Anteil kritischer Prozesse mit freigegebenem BCP
- KPI: Anteil IT-Services mit getesteter Recovery
- KPI: offene Massnahmen aus Übungen/Audits
- KPI: Aktualität Kontaktlisten und Stellvertretungen
- KPI: Lieferanten mit gültigem Continuity-Nachweis

Management-Nutzen

Wir nutzen das Reifegradmodell als Bewertungsraster für Policy, BIA, Risikoanalyse, Strategie, BCP, DRP, Supplier/Vendor Continuity, Übungen und Management-Reviews. Daraus entstehen ein realistisches Zielbild, Gap-Analyse, KPI-Set und eine priorisierte Verbesserungsroadmap.

Beratungsansatz

Das Management legt Zielreifegrade je BCM-Baustein, Reporting-Rhythmus, Steuerungskennzahlen, Risikotoleranz, Auditanspruch und Verbesserungsprioritäten fest. Damit wird entschieden, ob BCM nur dokumentiert, operativ eingeführt, regelmässig geübt oder als Managementsystem gesteuert wird.

Ergebnisqualität

Nachweisfähig sind Reifegradbewertung, KPI-Dashboard, Gap-Liste, Auditnachweise, Management-Review-Protokolle und Massnahmenstatus. Die Bewertung wird periodisch wiederholt und mit Übungen, Audits, Incidents, Prozessänderungen sowie strategischen Planungszyklen abgeglichen.

Workshop- und Interviewleitfaden

Die folgenden Leitfragen unterstützen strukturierte Interviews mit Geschäftsbereichen, IT, Einkauf, HR, Facility, Kommunikation, Legal/Compliance und Krisenmanagement. Sie sind als Arbeitshilfe gedacht und können direkt in Scribus an Kundensituation, Branche und Projektumfang angepasst werden.

BIA-Fragen

Welche Leistungen müssen zwingend erbracht werden? Welche Kunden, Behörden oder Stakeholder sind betroffen? Welche finanziellen, regulatorischen, operativen oder reputationsbezogenen Folgen entstehen nach 4 Stunden, 1 Tag, 3 Tagen oder 1 Woche? Welche Ressourcen, IT-Services, Daten, Räume, Lieferanten und Schlüsselpersonen werden benötigt?

Strategiefragen

Welche Ersatzverfahren sind realistisch? Können Leistungen reduziert, verschoben, manuell erbracht oder an andere Standorte verlagert werden? Welche Investitionen oder Verträge sind nötig? Welche Restrisiken akzeptiert die Geschäftsleitung?

BCP-/DRP-Fragen

Wer alarmiert wen? Wann wird eskaliert? Welche Sofortmassnahmen gelten? Welche Schritte führen zum Notbetrieb? Welche Wiederanlaufreihenfolge gilt? Welche Kontaktlisten und Kommunikationskanäle sind verfügbar? Welche technischen Voraussetzungen müssen vorliegen?

Übungsfragen

Welche Ziele verfolgt die Übung? Welches Szenario prüft die grössten Unsicherheiten? Welche Entscheidungen müssen geübt werden? Welche Beobachtungskriterien gelten? Wie werden Massnahmen erfasst und nachverfolgt?

Management-Checkliste

- □ Jeder Workshop hat Ziel, Agenda, Teilnehmende, Rollen und erwartete Ergebnisse.
- □ Vorlagen werden vorab verteilt und nach dem Workshop konsolidiert.
- □ Entscheide, Annahmen und offene Punkte werden sichtbar dokumentiert.
- □ Ergebnisse werden validiert, freigegeben und in Roadmap oder Pläne übertragen.

Management-Nutzen

Wir strukturieren Workshops und Interviews so, dass BIA-, Strategie-, BCP-/DRP- und Übungsfragen zu belastbaren Ergebnissen führen. Teilnehmende, Agenda, Vorlagen und erwartete Outputs werden vorab definiert; Annahmen, Entscheide und offene Punkte werden sichtbar dokumentiert.

Beratungsansatz

Projektleitung und Management bestätigen Workshop-Scope, Teilnehmende, Ergebnisformat, Prioritäten und Validierungsweg. Nach den Workshops werden offene Annahmen, kritische Abhängigkeiten, Strategieoptionen, Ressourcenkonflikte und nächste Umsetzungsschritte entschieden.

Ergebnisqualität

Nachweisfähig sind Agenda, Teilnehmerliste, Interviewnotizen, ausgefüllte Vorlagen, Entscheidprotokoll, offene Punkte und validierte Ergebnisse. Die Inhalte werden in BIA, Strategie, BCP, DRP, Roadmap oder Massnahmenliste überführt und versioniert weitergepflegt.

RM Risk Management AG
Business-Resilienz & GRC Consultants

Ihr nächster Schritt

RM Risk Management AG | Business Continuity & Resilienz

Starten Sie mit einem strukturierten Erstgespräch, einem Quick Assessment oder einem fokussierten Management-Workshop. Daraus entstehen eine belastbare Standortbestimmung, eine priorisierte Roadmap und ein klarer Entscheid über die nächsten Umsetzungsschritte.

Leistungsfelder für den Einstieg

- □ BCM, BIA, Business Continuity Strategie und Business Continuity Pläne
- □ IT Service Continuity Management, Service Impact Analyse und Disaster Recovery Plan
- □ Supplier Continuity, Vendor Continuity und Risk Rating
- □ Krisenmanagement, Krisenkommunikation, Schulungen und Übungen
- □ ISO-22301-Coaching, Gap-Analyse, Auditfähigkeit und kontinuierliche Verbesserung

RM Risk Management AG, Hertistrasse 25, 8304 Wallisellen / Zürich | Tel. +41 44 360 40 40
business-continuity-resilienz.ch