RM Risk Management AG
Business-Resilienz & GRC Consultants

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

Checkliste: Ist Ihr BCM wirksam?

Praxisorientierte Selbsteinschätzung für Business Continuity Management, BCM-Prozess und organisatorische Resilienz

Diese Checkliste unterstützt Geschäftsleitung, BCM-Verantwortliche, Risikomanagement, IT, Compliance und Fachbereiche bei der Beurteilung, ob das Business Continuity Management nicht nur dokumentiert, sondern im Ernstfall auch wirksam ist. Bewertet werden Governance, Business Impact Analyse, Risikoanalyse, BCM-Strategie, Business Continuity Pläne, Übungen, Tests und kontinuierliche Verbesserung.

So verwenden Sie die Checkliste

Bewerten Sie jede Prüffrage mit 0, 1 oder 2 Punkten. Entscheidend ist nicht nur, ob ein Dokument existiert, sondern ob die Massnahme aktuell, bekannt, geübt und im Ereignisfall anwendbar ist.

Bewertung	Bedeutung
0	Nicht vorhanden, nicht dokumentiert oder nicht nachweisbar.
1	Teilweise vorhanden, aber unvollständig, nicht aktuell, nicht bekannt oder nicht getestet.
2	Vollständig umgesetzt, aktuell, freigegeben, bekannt und praktisch getestet.
N/A	Nicht anwendbar. Bei der Prozentberechnung aus dem Maximalwert herausnehmen.

Hinweis: Eine hohe Punktzahl ersetzt keine BCM-Übung, kein Audit und keine fachliche Prüfung. Sie zeigt jedoch, wo Handlungsbedarf besteht und welche Themen priorisiert werden sollten.

1. Governance, Policy und BCM-Organisation

Markieren Sie pro Frage den passenden Reifegrad und notieren Sie Nachweise, Lücken oder nächste Massnahmen.

Nr.	Prüffrage	Möglicher Nachweis	0	1	2	N/A	Notizen / Massnahmen
1.1	Gibt es eine von der Geschäftsleitung genehmigte BCM Policy mit Ziel, Geltungsbereich und Mindestanforderungen?	BCM Policy, Beschluss, Review-Datum					
1.2	Sind Rollen, Verantwortlichkeiten und Stellvertretungen für Business Continuity Management klar definiert?	RACI, Funktionsbeschreibungen, Organigramm					
1.3	Ist BCM in Risikomanagement, Krisenmanagement, Informationssicherheit, IT und Compliance eingebunden?	Schnittstellen, Governance-Gremien, Prozesslandkarte					
1.4	Gibt es einen BCM-Verantwortlichen mit ausreichendem Mandat, Ressourcen und direktem Zugang zur Führung?	Mandat, Budget, Reporting-Linie					
1.5	Sind BCM-Ziele messbar definiert und werden sie regelmässig an die Geschäftsleitung berichtet?	Ziele, KPIs, Management Reporting					
1.6	Ist der Geltungsbereich des BCM aktuell und umfasst kritische Standorte, Geschäftsprozesse, IT-Systeme und Dienstleister?	Scope-Dokument, Standort- und Prozessübersicht					

2. Business Impact Analyse (BIA)

Nr.	Prüffrage	Möglicher Nachweis	0	1	2	N/A	Notizen / Massnahmen
2.1	Wurde eine aktuelle Business Impact Analyse für alle relevanten Geschäftsbereiche durchgeführt?	BIA-Bericht, Interviewprotokolle, Freigaben					
2.2	Sind kritische Geschäftsprozesse eindeutig identifiziert und priorisiert?	Prozessliste, Kritikalitätsbewertung					
2.3	Sind maximale tolerierbare Ausfallzeiten, Wiederanlaufziele und Mindestleistungen dokumentiert?	MTPD, RTO, RPO, Minimalbetrieb					
2.4	Sind Auswirkungen eines Ausfalls finanziell, operativ, rechtlich, regulatorisch und reputationsbezogen bewertet?	Impact-Kriterien, Bewertungsskala					
2.5	Sind Abhängigkeiten zu Mitarbeitenden, IT, Daten, Gebäuden, Lieferanten und externen Dienstleistern erfasst?	Abhängigkeitsmatrix, Ressourcenübersicht					
2.6	Wurden die BIA-Ergebnisse durch Prozessverantwortliche und Führung validiert?	Freigaben, Workshop-Ergebnisse					

3. Risikoanalyse und relevante Szenarien

Nr.	Prüffrage	Möglicher Nachweis	0	1	2	N/A	Notizen / Massnahmen
3.1	Sind die wichtigsten Unterbrechungsszenarien für kritische Prozesse analysiert?	Szenariokatalog, Risikoregister					
3.2	Werden Cyberangriffe, IT-Ausfälle, Stromunterbrüche, Gebäudeausfall, Personalausfall und Lieferkettenstörungen berücksichtigt?	Risikoanalyse, Szenarioannahmen					
3.3	Sind bestehende Schutzmassnahmen und verbleibende Restrisiken transparent dokumentiert?	Kontrollmatrix, Massnahmenplan					
3.4	Sind Single Points of Failure in Organisation, Technik, Infrastruktur und Lieferkette bekannt?	SPOF-Liste, Abhängigkeitsanalyse					
3.5	Werden Risikoanalyse und BIA zusammengeführt, um Prioritäten für BCM-Massnahmen abzuleiten?	Priorisierung, Entscheidungsgrundlagen					

4. BCM-Strategie und Vorsorgemassnahmen

Nr.	Prüffrage	Möglicher Nachweis	0	1	2	N/A	Notizen / Massnahmen
4.1	Gibt es genehmigte BCM-Strategien für die Fortführung oder Wiederherstellung kritischer Prozesse?	Strategiedokument, Management-Entscheid					
4.2	Sind Notbetrieb, Ersatzverfahren und Wiederanlaufreihenfolge realistisch beschrieben?	Strategie, Prozessdokumentation					
4.3	Sind alternative Arbeitsorte, Homeoffice, Stellvertretungen und Schlüsselpersonenregelungen geplant?	Arbeitsplatzkonzept, Stellvertreterliste					
4.4	Sind Anforderungen an IT-Wiederherstellung, Datenverfügbarkeit und manuelle Ersatzprozesse abgestimmt?	ITSCM/DR-Konzept, RTO/RPO-Abgleich					
4.5	Gibt es Strategien für den Ausfall wichtiger Lieferanten, Dienstleister oder ausgelagerter Prozesse?	Supplier-Continuity-Konzept, Vertragsklauseln					
4.6	Sind Massnahmen wirtschaftlich angemessen und mit Geschäftsleitung, Fachbereichen und IT abgestimmt?	Kosten-Nutzen-Bewertung, Freigaben					

5. Business Continuity Pläne

Nr.	Prüffrage	Möglicher Nachweis	0	1	2	N/A	Notizen / Massnahmen
5.1	Existieren aktuelle Business Continuity Pläne für alle kritischen Prozesse und Standorte?	BCP-Verzeichnis, Versionskontrolle					
5.2	Enthalten die Pläne klare Auslösekriterien, Eskalationswege, Verantwortlichkeiten und Sofortmassnahmen?	BCP, Alarmierungsprozess					
5.3	Sind Kontaktlisten, Entscheidungsbefugnisse und Stellvertretungen aktuell und ausserhalb der Primärsysteme verfügbar?	Kontaktlisten, Offline-Kopien					
5.4	Beschreiben die Pläne konkrete Schritte für Notbetrieb, Wiederanlauf und Rückkehr zum Normalbetrieb?	Checklisten, Wiederanlaufverfahren					
5.5	Sind Schnittstellen zu Krisenstab, Kommunikation, IT-Notfallmanagement, HR und Facility Management geregelt?	Schnittstellenbeschreibung, Ablaufdiagramme					
5.6	Sind die Pläne für Anwender verständlich, schlank und im Ereignisfall rasch nutzbar?	Praxistest, Feedback der Anwender					

6. Krisenmanagement und Kommunikation

Nr.	Prüffrage	Möglicher Nachweis	0	1	2	N/A	Notizen / Massnahmen
6.1	Ist geregelt, wann ein Ereignis vom Linienbetrieb ins Krisenmanagement eskaliert wird?	Eskalationskriterien, Alarmplan					
6.2	Sind Krisenstab, Entscheidungswege, Lagebildführung und Protokollierung festgelegt?	Krisenhandbuch, Rollenbeschreibungen					
6.3	Gibt es vorbereitete Kommunikationswege und Vorlagen für Mitarbeitende, Kunden, Lieferanten, Medien und Behörden?	Kommunikationsplan, Textbausteine					
6.4	Sind alternative Kommunikationskanäle vorhanden, falls E-Mail, Telefonie oder Kollaborationstools ausfallen?	Notfallkanäle, Verteiler, Tests					
6.5	Sind Meldepflichten, regulatorische Anforderungen und vertragliche Informationspflichten bekannt?	Compliance-Matrix, Meldeprozess					

7. Übungen, Tests und Schulung

Nr.	Prüffrage	Möglicher Nachweis	0	1	2	N/A	Notizen / Massnahmen
7.1	Gibt es einen jährlichen Übungs- und Testplan für BCM, Krisenmanagement und IT-Wiederherstellung?	Testplan, Übungskalender					
7.2	Werden Tabletop-Übungen, funktionale Tests und technische Wiederherstellungstests regelmässig durchgeführt?	Übungsberichte, Testprotokolle					
7.3	Prüfen Übungen realistische Szenarien und die Zusammenarbeit mehrerer Bereiche?	Szenariobeschreibung, Teilnehmerliste					
7.4	Werden definierte Wiederanlaufzeiten, Kommunikationswege und Entscheidungsprozesse praktisch getestet?	Testergebnisse, Zeitmessungen					
7.5	Werden Mitarbeitende und Schlüsselpersonen regelmässig zu ihren BCM-Aufgaben geschult?	Schulungsnachweise, Awareness-Unterlagen					
7.6	Führen Übungen zu konkreten Verbesserungsmassnahmen mit Verantwortlichen und Fristen?	Lessons Learned, Massnahmen-Tracking					

8. IT, Daten, Lieferanten und weitere Abhängigkeiten

Nr.	Prüffrage	Möglicher Nachweis	0	1	2	N/A	Notizen / Massnahmen
8.1	Sind kritische IT-Systeme, Daten, Schnittstellen und Wiederherstellungsabhängigkeiten mit der BIA abgeglichen?	Applikationslandkarte, DR-Anforderungen					
8.2	Sind Backups, Wiederherstellung, Notfallzugriffe und Cyber-Resilienz-Massnahmen getestet?	Backup-Tests, Restore-Protokolle					
8.3	Sind ausgelagerte Leistungen und Cloud-Dienste in BCM-Planung, Tests und Verträge eingebunden?	Provider-Nachweise, SLAs, Exit-Pläne					
8.4	Gibt es alternative Lieferanten, Mindestlager, Ersatzprozesse oder andere Massnahmen für kritische Lieferketten?	Lieferantenstrategie, Lagerkonzept					
8.5	Sind physische Standorte, Zutritt, Energie, Netzwerk, Transport und Arbeitsmittel in den Szenarien berücksichtigt?	Facility-Plan, Standortanalyse					

9. Review, Audit und kontinuierliche Verbesserung

Nr.	Prüffrage	Möglicher Nachweis	0	1	2	N/A	Notizen / Massnahmen
9.1	Werden BCM Policy, BIA, Risikoanalyse, Strategien und Pläne mindestens jährlich oder anlassbezogen überprüft?	Review-Plan, Änderungshistorie					
9.2	Gibt es klare Auslöser für Aktualisierungen, z.B. neue Prozesse, IT-Systeme, Standorte, Lieferanten oder regulatorische Anforderungen?	Change-Prozess, BCM-Kriterien					
9.3	Werden Ergebnisse aus Übungen, Audits, Incidents und Near Misses systematisch ausgewertet?	Lessons Learned, Auditberichte					
9.4	Sind Korrektur- und Verbesserungsmassnahmen priorisiert, terminiert und bis zum Abschluss nachverfolgt?	Massnahmenregister, Statusreporting					
9.5	Erhält die Geschäftsleitung regelmässig ein BCM-Reporting mit Risiken, Reifegrad, Tests und offenen Massnahmen?	Management Review, Dashboard					
9.6	Ist das BCM auch bei organisatorischen Veränderungen stabil und wird es als laufender Managementprozess gelebt?	Nachweise, Governance, Kultur					

Auswertung und Priorisierung

Übertragen Sie die Punkte je Bereich in die folgende Übersicht. Ziehen Sie N/A-Fragen vom Maximalwert ab und berechnen Sie den Reifegrad in Prozent.

Bereich	Max. Punkte	Erreichte Punkte	Wichtigste Lücken / nächste Massnahmen
Governance, Policy und BCM-Organisation	12		
Business Impact Analyse (BIA)	12		
Risikoanalyse und relevante Szenarien	10		
BCM-Strategie und Vorsorgemassnahmen	12		
Business Continuity Pläne	12		
Krisenmanagement und Kommunikation	10		
Übungen, Tests und Schulung	12		
IT, Daten, Lieferanten und weitere Abhängigkeiten	10		
Review, Audit und kontinuierliche Verbesserung	12		
Total	**102**		

Formel: erreichte Punkte / angepasste Maximalpunkte x 100 = BCM-Reifegrad in Prozent.

Interpretation des Ergebnisses

Ergebnis	Interpretation
0-40 %	Kritischer Handlungsbedarf: BCM ist nur punktuell vorhanden oder im Ereignisfall nicht belastbar.
41-70 %	Grundlagen vorhanden: zentrale Elemente müssen ergänzt, aktualisiert oder getestet werden.
71-85 %	Solide Basis: BCM ist weitgehend umgesetzt, sollte aber gezielt gehärtet und geübt werden.
86-100 %	Hoher Reifegrad: BCM ist strukturiert, aktuell, getestet und wird kontinuierlich verbessert.

Nächste Schritte

1. Kritische Lücken priorisieren: zuerst Themen mit hohem Einfluss auf Menschen, Kunden, Compliance, Liquidität und Reputation bearbeiten.
2. Nachweise sichern: BCM sollte anhand freigegebener Dokumente, Tests, Übungsberichte und Management-Entscheide belegbar sein.
3. Pläne praktisch testen: ein Business Continuity Plan ist erst belastbar, wenn Rollen, Kommunikation und Wiederanlauf unter realistischen Bedingungen geübt wurden.
4. Kontinuierlich verbessern: Erkenntnisse aus Übungen, Incidents, Audits und Veränderungen im Unternehmen systematisch in das BCM zurückführen.

Diese Checkliste dient als praxisorientierter Einstieg. Für eine belastbare Beurteilung sollten Ergebnisse mit Übungen, Nachweisen, Interviews und Management Reviews validiert werden.