

MODUL · BCM

Modul Business Continuity Management (BCM)

Business Continuity Management nach BSI 200-4 und ISO 22301

Produktversion 2026.08.19 · Handbuch-Revision 1.0

Stand 19.08.2026 · Plattform .NET 10 / Windows Server

ID-29 BCM

Modul Business Continuity Management (BCM)

Was passiert, wenn das Rechenzentrum brennt, ein Verschlüsselungsangriff die Systeme lahmlegt oder für Wochen zu viele Mitarbeitende gleichzeitig ausfallen? Solche Ereignisse sind selten, aber wenn sie eintreten, entscheidet sich in Stunden, ob eine Organisation handlungsfähig bleibt. Wer dann erst anfängt zu überlegen, wer was tun soll, verliert wertvolle Zeit.

Business Continuity Management (BCM), auf Deutsch die Steuerung der Geschäftsfortführung, ist die Vorsorge für genau solche Fälle. Der Grundgedanke: erst herausfinden, welche Geschäftsprozesse wie schnell wieder laufen müssen (die Business-Impact-Analyse), dann Rollen, Pläne und Zuständigkeiten für den Notfall festlegen und das Ganze in Übungen erproben. Das Modul folgt den anerkannten Standards BSI 200-4 und ISO 22301. Es kümmert sich um die organisatorische Seite eines Notfalls; den technischen Wiederanlauf der Systeme behandelt die DR-Planung (ID-30).

INHALT

- 1 Zweck & Nutzen
- 2 Business-Impact-Analyse (BIA)
- 3 Notfallorganisation (BAO)
- 4 Notfallpläne
- 5 IT-Notfallhandbuch (generiert)
- 6 Übungen & CAPA
- 7 Abgrenzung
- 8 Rollen & Rechte (Auszug)
- Verwandte Themen

1 Zweck & Nutzen

- Kritische Geschäftsprozesse und ihre Ausfalltoleranz kennen.
- Vorbereitung auf Notfälle (Rollen, Pläne, Übungen).
- Nachweise für Audits.

2 Business-Impact-Analyse (BIA)

Die **BIA** bewertet je Geschäftsprozess die Kritikalität und Zeitziele:

Abbildung 1 zeigt die Analyse mit Zeitzielen und der Prüfung auf Zeitketten-Konflikte.

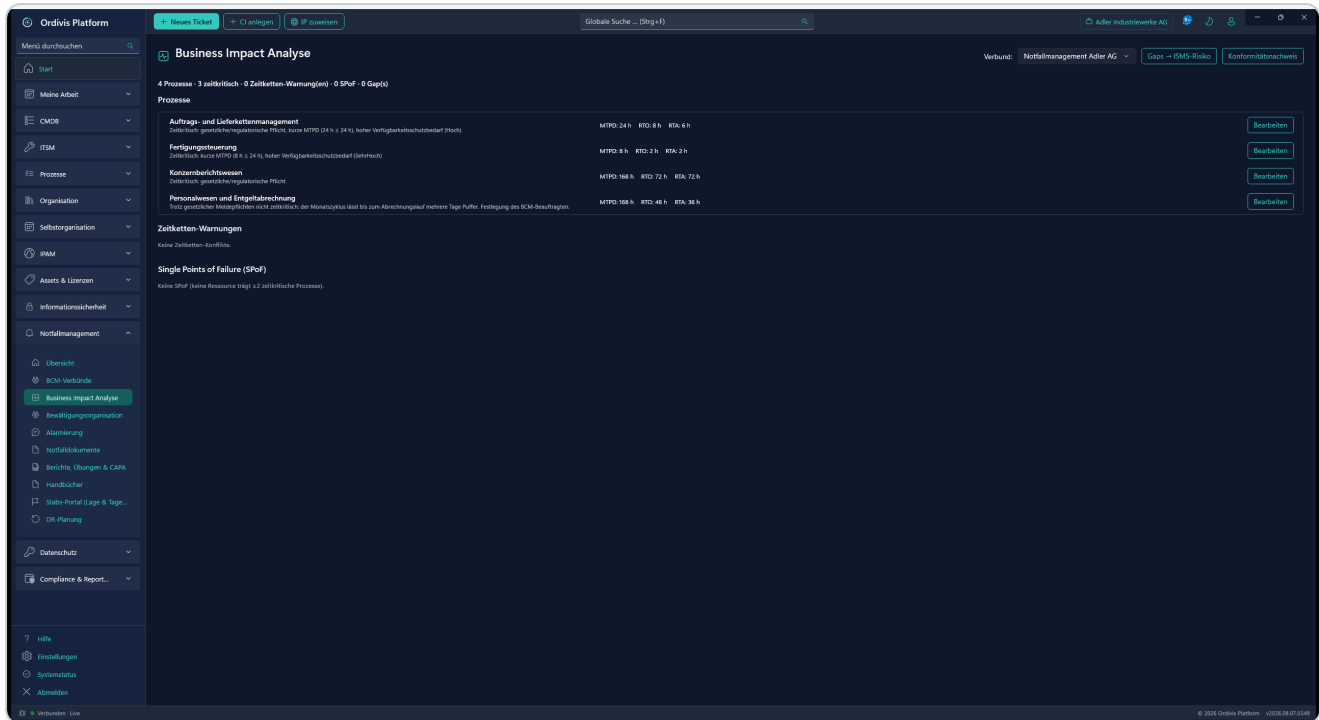


Abb. 1 – Business-Impact-Analyse: je Geschäftsprozess Zeitkritikalität, MTPD, RTO/RTA sowie Prüfung auf Zeitketten-Konflikte und Single Points of Failure.

- MTPD – maximal tolerierbare Ausfallzeit.
- RTO/RPO – Wiederanlauf- und Datenverlustziele.
- Verfügbarkeitsanforderung.

Wichtig: Die Zeitkritikalität kommt aus dem **Vorfilter** (`BcmBiaVorfilter`) und wird **live** berechnet (Pflicht ODER $MTPD \leq 24\text{ h}$ ODER Verfügbarkeit hoch). Ein gespeicherter Wert zählt nur bei manueller Übersteuerung (`IsManualOverride`) – sonst weichen Berichte von der BIA-Seite ab.

3 Notfallorganisation (BAO)

 **Nur im Client:** *Notfallmanagement* ▶ *Bewältigungsorganisation* ·  `bcm.plan.manage` — Das Portal zeigt die Aufstellung im *BCM-Arbeitsplatz*, besetzt die Rollen aber nicht.

Definieren Sie die **Besondere Aufbauorganisation** für den Notfall: Rollen (Krisenstab, Notfallbeauftragte), Erreichbarkeiten und Eskalationswege.

 **Pflichtreihenfolge** — eine Rolle ohne Erreichbarkeit ist im Ernstfall keine. Besetzen Sie deshalb erst die Rolle und hinterlegen Sie unmittelbar danach, wie die Person nachts erreicht wird.

1. Öffnen Sie *Notfallmanagement* ▶ *Bewältigungsorganisation*.
2. Legen Sie die benötigten **Rollen** an (Krisenstabsleitung, Notfallbeauftragte, Sprecher ...).
3. Besetzen Sie jede Rolle mit einer Person **und** einer Vertretung.

4. Hinterlegen Sie je Person die **Erreichbarkeit außerhalb der Dienstzeit** – die dienstliche Durchwahl hilft um drei Uhr nachts nicht.
5. Legen Sie den **Eskalationsweg** fest: wer wen in welcher Reihenfolge alarmiert.
6. Speichern Sie.

✓ **Ergebnis:** Die Aufstellung steht und geht in das generierte IT-Notfallhandbuch ein (Abschnitt 5).

Achtung: Prüfen Sie die Erreichbarkeiten mindestens jährlich. Eine BAO mit der Mobilnummer eines vor zwei Jahren ausgeschiedenen Kollegen ist im Ernstfall nicht bloß nutzlos – sie kostet die Minuten, in denen jemand vergeblich anruft.

Abbildung 2 zeigt eine solche Aufstellung.

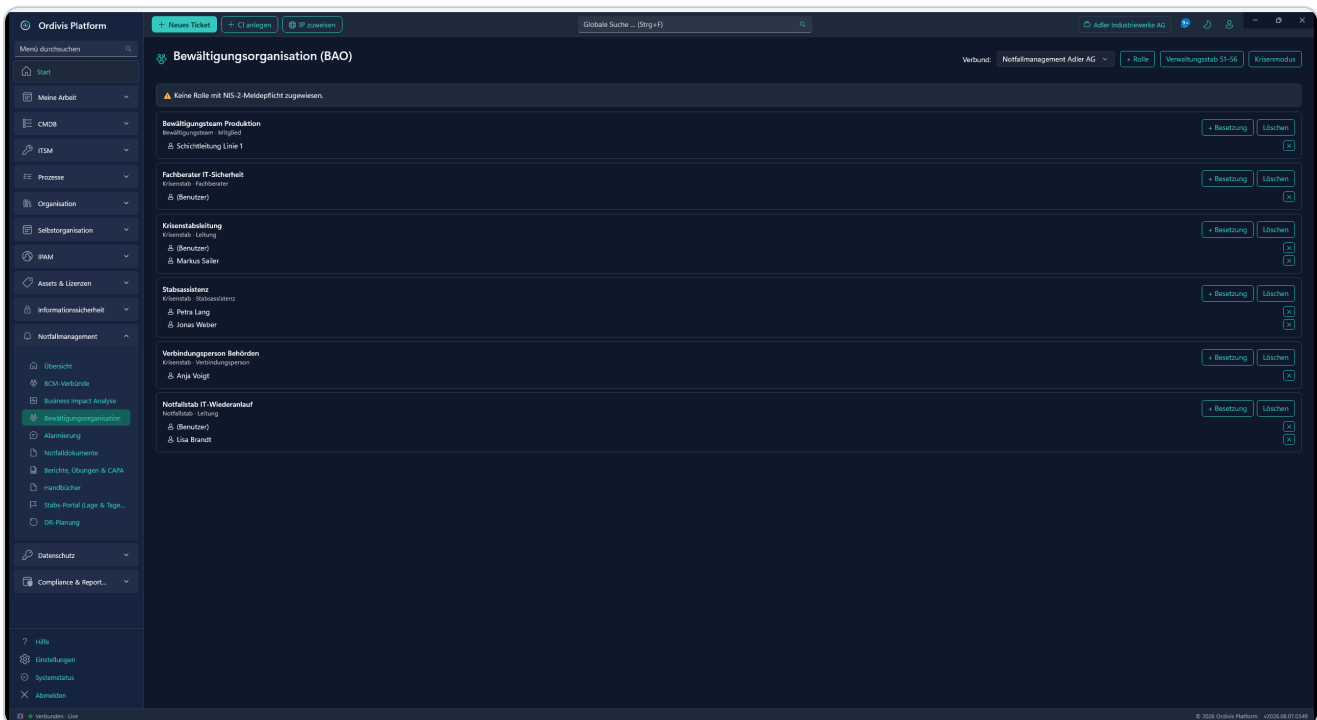


Abb. 2 – Bewältigungsorganisation (BAO): Krisenstab- und Notfallrollen mit den zugewiesenen Personen.

4 Notfallpläne

Erstellen Sie Pläne je Szenario (Ausfall Rechenzentrum, Personalausfall ...) mit klaren Schritten, Verantwortlichen und benötigten Ressourcen. Pläne verknüpfen sich mit CIs/Diensten aus der CMDB.

5 IT-Notfallhandbuch (generiert)

Ordvis Platform erzeugt aus den Daten, die Sie in diesem Modul ohnehin pflegen, ein vollständiges **IT-Notfallhandbuch nach BSI 200-4** – Sie schreiben es nicht, Sie geben den Verbund an.

Erzeugen: Notfallhandbuch für einen BCM-Verbund generieren. Es entsteht ein versioniertes Handbuch im Entwurf mit sieben Kapiteln:

Kapitel	Woher der Inhalt kommt
Zweck & Geltungsbereich	Verbund, Reifegrad, Lage; zeitkritische Prozesse mit MTPD/RTO/RPO
Notfallorganisation (BAO)	Rollen und Besetzung inkl. Vertretung; Hinweis auf fehlende Vertretung und Meldepflicht
Alarmierung & Eskalation	Alarmierungskontakte je Eskalationsstufe (nur aktive)
Sofortmaßnahmen	Checklisten der Kategorie „Notfall“ aus der Checklisten-Engine
Kommunikationsplan	Kommunikations- und Warnkanäle des Verbunds
Kontaktverzeichnis	alle Kontakte inkl. Organisation (intern/Dienstleister)
Notfalldokumente	die freigegebenen Dokumente der Notfalldokumenten-Bibliothek

Der entscheidende Punkt – es wird nichts kopiert. Die Kapitel halten nur einen Verweis auf ihre Quelle und werden bei **jedem Abruf neu aufgelöst**. Ändern Sie eine Rufnummer in der Alarmierungsliste, steht sie sofort im Handbuch – ohne es neu zu erzeugen. Damit kann ein Notfallhandbuch nicht unbemerkt veralten, und es gibt keine doppelte Pflege.

Hinweis: Lässt sich eine Quelle nicht mehr auflösen (z. B. gelöschter Verbund), weist das Kapitel dies **sichtbar** aus, statt still leer zu bleiben. Eine unbemerkte Lücke im Notfallhandbuch wäre gefährlicher als ein Hinweis.

Versionieren & freigeben: Ein Handbuch ist zunächst **Entwurf** und bearbeitbar. Mit der **Freigabe** wird der Stand eingefroren und gegen Änderungen geschützt – das ist der Stand, den Sie einer Prüfung vorlegen. Für eine Überarbeitung öffnen Sie den freigegebenen Stand wieder; dabei entsteht automatisch die **nächste Version**. Dynamische Kapitel zeigen auch im freigegebenen Handbuch weiterhin den Live-Stand ihrer Quellen – gerade Notfallkontakte müssen aktuell sein.

Betriebshandbücher und Wiederanlaufpläne nutzen dasselbe Handbuch-Gerüst; deren Generatoren folgen.

6 Übungen & CAPA

Planen und protokollieren Sie **Übungen** (Tests der Pläne). Aus Erkenntnissen entstehen **Korrektur- und Vorbeugemaßnahmen (CAPA)**, deren Umsetzung verfolgt wird.

7 Abgrenzung

- **BCM (dieses Modul):** organisatorische Geschäftsfortführung.
- **DR-Planung (ID-30):** technischer Wiederanlauf von IT-Systemen.
- **ISMS (ID-28):** Sicherheitsanforderungen und Risiken.

8 Rollen & Rechte (Auszug)

Recht	Erlaubt
bcm.plan.read / bcm.report.read / bcm.risk.read	Pläne, Berichte und Risiken ansehen
bcm.bia.manage / bcm.plan.manage / bcm.exercise.manage	BIA, Pläne und Übungen pflegen
bcm.scope.manage / bcm.org.manage	Geltungsbereich und Krisenorganisation verwalten
bcm.crisis.operate	Krisenmodus bedienen (Stab, Einsatztagebuch)
handbook.read	Handbücher lesen (Betrieb/Notfall/Wiederaufbau)
handbook.manage	Handbücher generieren und pflegen
handbook.approve	Handbuch freigeben (Entwurf → freigegebener Stand)

Verwandte Themen

- ID-28 – Modul Informationssicherheit (ISMS) – Informationssicherheit als Rahmen
- ID-30 – Modul Notfall- & Wiederaufbauplanung (DR) – der technische Wiederaufbau
- ID-29a – Modul Checklisten – Übungen und Prüfungen als Checkliste
- ID-33 – Modul Organisation & Geschäftsverteilungsplan – Prozesse und Federführung für die BIA