

MODUL · DR-PLANUNG

Modul Notfall- & Wiederanlaufplanung (DR)

Technischer Wiederanlauf von IT-Systemen nach einem Ausfall

Produktversion 2026.08.19 · Handbuch-Revision 1.0

Stand 19.08.2026 · Plattform .NET 10 / Windows Server

ID-30 DR-Planung

Modul Notfall- & Wiederanlaufplanung (DR)

Wenn ein Server oder ein ganzes System ausgefallen ist, zählt jede Minute, und niemand sollte im Ernstfall erst überlegen müssen, in welcher Reihenfolge was wieder hochzufahren ist. Fehlt ein getesteter Plan, wird aus einer beherrschbaren Störung schnell ein langer Ausfall, weil Wissen fehlt, Abhängigkeiten übersehen werden oder eine Sicherung sich als unbrauchbar erweist.

Disaster Recovery (DR), also die Wiederherstellung nach einem Notfall, ist der technische Fahrplan für den Wiederanlauf der IT. Ein DR-Plan beschreibt je Ausfallszenario die konkreten Schritte, die richtige Reihenfolge, die Verantwortlichen und die betroffenen Systeme. Während das BCM (ID-29) die organisatorische Frage beantwortet „Wie bleibt das Geschäft handlungsfähig?“, beantwortet die DR-Planung die technische: „Wie bekommen wir diese Systeme wieder zum Laufen, und schnell genug?“.

INHALT

- 1 Zweck & Nutzen
- 2 Einen DR-Plan anlegen
- 3 Bezug zu CIs & Diensten
- 4 Zeitziele (RTO/RPO)
- 5 Test & Pflege
- 6 Rollen & Rechte (Auszug)
- Verwandte Themen

1 Zweck & Nutzen

- Klare, getestete Schritte zur Wiederherstellung kritischer Systeme.
- Bezug zwischen Wiederanlaufplänen und konkreten CIs/Diensten.
- Einhaltung von RTO/RPO aus der BIA.

2 Einen DR-Plan anlegen

 **Nur im Client:** *Notfallmanagement* ▶ *DR-Planung* ▶ *Neuer Plan* ·  *dr.manage* — Das Portal zeigt die Pläne unter *Notfallmanagement* ▶ *DR-Pläne* an und nimmt Testnachweise entgegen (Abschnitt 5), legt aber keine Pläne an.

Voraussetzung: Die betroffenen Systeme sind als **CI** in der CMDB erfasst (ID-21). Ohne CI lässt sich weder die Verknüpfung noch die abgeleitete Reihenfolge herstellen.

 **Pflichtreihenfolge** — die vorgeschlagene Wiederanlaufreihenfolge (Abschnitt 3) entsteht aus den CMDB-Beziehungen der **verknüpften** Systeme. Verknüpfen Sie deshalb erst die CIs und ordnen Sie danach die Schritte, nicht umgekehrt.

1. Öffnen Sie *Notfallmanagement* ▶ *DR-Planung*.

2. Klicken Sie auf *Neuer Plan*.
3. Benennen Sie das **Szenario** so, wie es im Ernstfall gerufen wird – „Ausfall Datenbank-Server“, nicht „Plan 3“.
4. Verknüpfen Sie die betroffenen **CI**s/**Dienste** aus der CMDB.
5. Erfassen Sie die **Wiederanlaufschritte** – je Schritt Verantwortliche, veranschlagte Dauer und Voraussetzungen.
6. Tragen Sie **RTO** und **RPO** aus der BIA ein (Abschnitt 4).
7. Speichern Sie.

✅ **Ergebnis:** Der Plan steht in der Liste mit *Plan*, *Tier*, *RTO*, *RPO* und *Zuletzt getestet*. Solange kein Test dokumentiert ist, steht dort *nie getestet* – und das ist die ehrlichste Angabe, die die Liste machen kann.

Tipp: Schreiben Sie die Schritte so, dass sie um drei Uhr nachts von jemandem ausgeführt werden können, der das System nicht gebaut hat. Alles, was „ist ja klar“ ist, ist es dann nicht.

3 Bezug zu CI & Diensten

 **Client:** *Notfallmanagement* ▶ *DR-Planung*, Plan öffnen ·  **Portal:** *Notfallmanagement* ▶ *DR-Pläne* ·  *dr.read*

Durch die Verknüpfung mit der CMDB wissen Sie im Ernstfall genau, welche Systeme betroffen sind und in welcher Reihenfolge sie wiederhergestellt werden müssen (Abhängigkeiten zuerst).

Die vorgeschlagene Reihenfolge leitet Ordavis Plattform aus den CMDB-Beziehungen der verknüpften Systeme ab: Was von wenig anderem abhängt, steht vorn. Lässt sich für ein System keine Abhängigkeit ermitteln – etwa weil das CI zwischenzeitlich entfernt wurde –, wird es **ans Ende gestellt und als ungeklärt gekennzeichnet**, nicht an den Anfang. Der Unterschied ist im Ernstfall entscheidend: „keine Abhängigkeiten bekannt“ heißt nicht „hängt von nichts ab“. Prüfen Sie solche Einträge, bevor Sie der Reihenfolge folgen.

So prüfen Sie die vorgeschlagene Reihenfolge:

 **Pflichtreihenfolge** — sehen Sie zuerst die als *ungeklärt* gekennzeichneten Einträge durch. Erst danach hat die übrige Reihenfolge Aussagekraft.

1. Öffnen Sie den Plan.
2. Nehmen Sie sich jeden als **ungeklärt** gekennzeichneten Eintrag vor.
3. Prüfen Sie in der CMDB, ob das CI noch existiert und seine Beziehungen gepflegt sind (ID-21).
4. Ergänzen Sie fehlende Beziehungen.
5. Öffnen Sie den Plan erneut – die Reihenfolge wird neu abgeleitet.

✅ **Ergebnis:** Kein Eintrag steht mehr auf *ungeklärt*, und der Reihenfolge lässt sich im Notfall folgen, ohne sie zu hinterfragen.

4 Zeitziele (RTO/RPO)

Übernehmen Sie **RTO** (Wiederanlaufzeit) und **RPO** (tolerierbarer Datenverlust) aus der BIA und prüfen Sie, ob die geplanten Schritte diese Ziele einhalten.

 **Nur im Client:** *Notfallmanagement* ▶ *DR-Planung*, Plan öffnen ·  *dr.manage*

 **Pflichtreihenfolge** — die BIA steht vor dem DR-Plan. RTO und RPO sind eine fachliche Festlegung des Geschäfts (ID-29), keine technische Schätzung. Wer sie im DR-Plan erfindet, dokumentiert seinen Wunsch, nicht die Anforderung.

1. Schlagen Sie RTO und RPO des betroffenen Prozesses in der BIA nach (ID-29).
2. Tragen Sie beide Werte im DR-Plan ein.
3. Addieren Sie die veranschlagten Dauern Ihrer Wiederanlaufschritte.
4. Vergleichen Sie die Summe mit dem RTO.

 **Ergebnis:** Entweder passt der Plan – oder Sie haben schwarz auf weiß eine Lücke, die Sie melden können, bevor sie im Ernstfall auffällt.

Achtung: Ein RPO von vier Stunden verlangt eine Sicherung mindestens alle vier Stunden. Der DR-Plan ist der Ort, an dem diese Rechnung aufgeht oder nicht – prüfen Sie sie gegen den tatsächlichen Sicherungsplan (ID-35).

5 Test & Pflege

 **Client:** *Notfallmanagement* ▶ *DR-Planung*, Plan öffnen ·  **Portal:** *Notfallmanagement* ▶ *DR-Pläne* ▶ *Test dokumentieren* ·  *dr.manage*

Ein Plan ist nur so gut wie sein letzter Test. Nach jedem Test – ob Übung oder Ernstfall – gehört das Ergebnis in den Plan:

1. Öffnen Sie *DR-Pläne* und suchen Sie den geprüften Plan.
2. Klicken Sie auf *Test dokumentieren*.
3. Tragen Sie das *Testdatum* ein.
4. Wählen Sie unter *Ergebnis* zwischen *Erfolgreich* und *Mit Mängeln*.
5. Halten Sie unter *Feststellungen* fest, was nicht funktioniert hat. **Auch bei „Erfolgreich“** – dort steht, was länger gedauert hat als geplant.
6. Klicken Sie auf *Speichern*.

 **Ergebnis:** Es erscheint *Test dokumentiert*. In der Spalte *Zuletzt getestet* steht das Datum; *nie getestet* verschwindet.

Tipp: Prüfen Sie DR-Pläne regelmäßig – verzahnt mit den BCM-Übungen (ID-29) – und aktualisieren Sie sie bei jeder Änderung an der Infrastruktur. Ein Plan, der auf einen Server zeigt, den es nicht mehr gibt, ist im Ernstfall schlimmer als kein Plan: Er kostet die ersten zwanzig Minuten.

Achtung: *Mit Mängeln* ist ein Ergebnis, kein Makel. Ein Plan, bei dem nie etwas auffällt, wurde entweder nie ernsthaft getestet oder das Ergebnis nicht ehrlich vermerkt – beides fällt im Audit auf und im Ernstfall auf die Füße.

6 Rollen & Rechte (Auszug)

Recht	Erlaubt
<code>dr.read</code>	Pläne ansehen
<code>dr.manage</code>	Pläne und Testergebnisse pflegen

Verwandte Themen

- ID-29 – Modul Business Continuity Management – die fachliche Fortführungsplanung darüber
- ID-50 – Betriebshandbuch – Installation & Serverbetrieb – Sicherung und Wiederherstellung in der Praxis
- ID-21 – Modul CMDB – Abhängigkeiten zwischen Systemen
- ID-29a – Modul Checklisten – Wiederanlauf als abhakbare Checkliste
- ID-35 – Modul Datensicherung – ob der RPO durch den Sicherungsplan gedeckt ist