Bennert
CONSULTING

Der DORA Findings-Navigator

Die 6 Cluster, in die jedes Finding fällt. Und wie Sie Ihre Nacharbeit priorisieren.

Mit Bewertungs-Matrix für Zeitaufwand und Komplexität. Mit Vorlage Findings-Tracking für den direkten Einsatz.

12 Seiten. Aus der Praxis der laufenden Nacharbeit bei mehreren Banken und Versicherern.

Herausgeber: Bennert Consulting

Stand: 2026

> **Bonus im Paket**
>
> Auf Seite 13 finden Sie eine direkt einsatzbereite Vorlage für das Findings-Tracking Ihrer internen Nacharbeit.

Wer sollte das lesen

Dieses Dokument richtet sich an Entscheider in regulierten Finanzunternehmen, die ihre erste DORA-Prüfung hinter sich haben und jetzt vor einer strukturierten Findings-Liste sitzen.

Lesen Sie dieses Dokument, wenn Sie:

- Geschäftsführung, Vorstand oder CFO einer Bank, Versicherung oder Leasinggesellschaft sind
- Leiter Compliance, Leiter Revision, Leiter Risikomanagement oder IT-Leitung sind
- DORA-Verantwortlicher oder Leiter Auslagerungsmanagement sind
- den Prüfbericht mit Findings auf dem Tisch haben und nicht wissen, womit anfangen
- die Nacharbeit nicht chaotisch parallel machen wollen, sondern strukturiert
- die nächste jährliche Prüfung vorbereitet angehen wollen

Was Sie nach 30 Minuten Lesezeit wissen:

- Die 6 Themencluster, in die jedes DORA-Finding fällt
- Die Bewertungs-Matrix für Zeitaufwand und Komplexität
- Welche Findings typischerweise Quick-Wins sind
- Eine Vorlage Findings-Tracking, die Sie sofort verwenden können

Inhalt

Seite	Thema
3	Warum strukturierte Nacharbeit jetzt der Hebel ist
4	Der Cluster-Rahmen im Überblick
5	Cluster 1: Risikomanagement
6	Cluster 2: Operative Informationssicherheit
7	Cluster 3: Umgang mit Sicherheitsvorfällen
8	Cluster 4: Notfallplanung
9	Cluster 5: Drittparteien-Steuerung
10	Cluster 6: Dokumentation und Nachweise
11	Die Bewertungs-Matrix: Zeitaufwand und Komplexität
13	Vorlage Findings-Tracking + Nächste Schritte

Warum strukturierte Nacharbeit jetzt der Hebel ist

Die Prüfung ist durch. Der Bericht liegt auf dem Tisch. 20 Findings, 80 Findings, 300 Findings – je nach Institut und Prüfungstiefe.

Jetzt beginnt der eigentlich schwierige Teil. Nicht die Prüfung selbst, sondern die Nacharbeit. Und die entscheidet, wie Sie aus dem nächsten Prüfzyklus herauskommen.

Drei Fehler sehen wir aktuell in deutschen Finanzinstituten immer wieder:

Fehler 1: Parallel-Bearbeitung ohne Priorisierung

Das Team bekommt die Liste und fängt an. Jeder nimmt sich Findings, die er kennt. Nach 6 Wochen sind 30 Findings abgearbeitet, aber die strukturellen Probleme sind offen. Der Wirtschaftsprüfer prüft im nächsten Zyklus genau diese Themen, die Sie verschoben haben.

Fehler 2: Alles als gleich wichtig behandeln

Eine fehlende Dokumentations-Aktualisierung und ein fehlender Drittparteien-Steuerungsprozess bekommen die gleiche Priorität. Das Team verbrennt Energie. Die einfachen Dinge ziehen sich, die komplexen Themen werden immer weiter geschoben.

Fehler 3: Keine Cluster-Logik

Jedes Finding wird als Einzelthema behandelt. Dabei haben viele Findings den gleichen Ursprung. Wenn Sie den strukturell lösen, verschwinden mehrere Findings gleichzeitig. Ohne Cluster-Logik verpassen Sie diese Synergien.

Was funktioniert

Strukturierte Nacharbeit beginnt mit drei Schritten:

1. **Clustering** der Findings nach Themenbereichen
2. **Bewertung** nach Zeitaufwand und Komplexität
3. **Priorisierung** nach Wirkung und Ressourceneinsatz

Die folgenden Seiten nehmen Sie durch die 6 Cluster, die wir in der Praxis sehen. Mit typischen Findings pro Cluster. Mit Zeit- und Komplexitäts-Bewertung. Mit konkreten Beispielen aus aktuellen Nacharbeiten.

Der Cluster-Rahmen im Überblick

Jedes DORA-Finding, das Sie erhalten, fällt in einen dieser 6 Cluster. Die Cluster sind nicht beliebig. Sie folgen der Struktur der DORA selbst und entsprechen den Prüfungs-Schwerpunkten der Wirtschaftsprüfer.

Cluster	Typische Findings	Zeitaufwand
1. Risikomanagement	Risiko-Rahmenwerk, Bewertungsmethoden, Management-Reporting	Mittel bis hoch
2. Operative Informationssicherheit	Zugriffe, Verschlüsselung, Tests, Schulung	Niedrig bis mittel
3. Umgang mit Sicherheitsvorfällen	Erkennung, Klassifikation, BaFin-Meldewege	Mittel
4. Notfallplanung	Wiederanlauf, Mindestversorgung, Übungen	Hoch
5. Drittparteien-Steuerung	Register, Verträge, Unter-Dienstleister, Ausstiegs-Strategien	Hoch
6. Dokumentation und Nachweise	Richtlinien, Protokolle, Reports, Aktualisierungen	Niedrig

Warum diese 6 Cluster

Diese Clusterung erlaubt drei Dinge:

Synergien nutzen. Findings innerhalb eines Clusters haben oft den gleichen Ursprung. Wer das Risiko-Rahmenwerk strukturell überarbeitet, löst in der Regel 4 bis 8 Findings auf einmal.

Ressourcen bündeln. Die Cluster haben unterschiedliche Ansprechpartner. Cluster 6 liegt oft beim Team Dokumentation, Cluster 5 beim Auslagerungsmanagement, Cluster 4 bei der IT. Ein sauber geclustertes Vorgehen vermeidet parallele Einzelgespräche.

Priorisieren. Dokumentations-Findings (Cluster 6) sind meist Quick-Wins. Drittparteien-Findings (Cluster 5) sind fast immer Langläufer. Wer das vorab sieht, plant realistisch.

Die folgenden 6 Seiten nehmen jeden Cluster einzeln durch. Mit Beispiel-Findings, Zeitaufwands-Bewertung und typischen Fallstricken.

Cluster 1: Risikomanagement

> **Was in diesem Cluster liegt:** Alle Findings, die sich auf das Rahmenwerk zur Steuerung Ihrer IT-Risiken beziehen. Vom Grundlagen-Dokument bis zum Vorstands-Reporting.

Typische Findings

- Das Risiko-Rahmenwerk ist älter als 12 Monate und wurde nicht überprüft
- Die Bewertungs-Methodik ist nicht schriftlich dokumentiert
- Neue Systeme oder Dienstleister sind nicht in die Bewertung eingeflossen
- Das Management-Reporting zum IT-Risiko-Status findet nicht regelmäßig statt
- Restrisiken sind nicht explizit von der Geschäftsleitung akzeptiert

Zeitaufwand und Komplexität

Dimension	Einordnung
Zeitaufwand	Mittel bis hoch (4 bis 12 Wochen)
Komplexität	Hoch (strategisch, berührt mehrere Bereiche)
Quick-Wins möglich?	Ja, bei reinen Dokumentations-Findings
Langläufer?	Ja, wenn Methodik-Anpassungen nötig sind

Der typische Fallstrick

Das Risiko-Rahmenwerk ist ein Grundlagen-Dokument. Wer es überarbeitet, löst viele Findings auf einen Schlag. Aber: Die Überarbeitung erfordert Abstimmung mit Vorstand, Revision, Compliance und IT. Das zieht sich ohne klare Projektleitung schnell auf 6 Monate.

Was wir in der Praxis empfehlen: Dieser Cluster gehört in die erste Prioritätsgruppe, aber nicht in die Selbstumsetzung. Hier zahlt sich externe Begleitung am stärksten aus, weil das Rahmenwerk drei Jahre hält und die Prüfungs-Grundlage für alles andere ist.

Cluster 2: Operative Informationssicherheit

> **Was in diesem Cluster liegt:** Alle Findings zu Zugriffsrechten, Verschlüsselung, Tests der Widerstandsfähigkeit und Schulungen.

Typische Findings

- Mehrfaktor-Authentisierung nicht bei allen privilegierten Zugriffen aktiv
- Berechtigungsrevision länger als 12 Monate zurück
- Verschlüsselungs-Standards nicht durchgängig dokumentiert
- Penetrationstests aus dem letzten Jahr, aber Nacharbeit offen
- Schulungen für privilegierte Nutzer nicht dokumentiert oder veraltet

Zeitaufwand und Komplexität

Dimension	Einordnung
Zeitaufwand	Niedrig bis mittel (2 bis 8 Wochen)
Komplexität	Mittel (technisch und organisatorisch)
Quick-Wins möglich?	Ja, viele davon
Langläufer?	Selten

Der typische Fallstrick

Diese Findings wirken einzeln einfach, aber sie summieren sich. Eine fehlende Mehrfaktor-Authentisierung hier, eine veraltete Schulungsliste dort. Wer sie einzeln parallel abarbeitet, bindet Ressourcen über 3 bis 4 Monate ohne Struktur.

Was wir in der Praxis empfehlen: Dieser Cluster eignet sich gut für eine Bündelung. Eine klare Arbeitsgruppe, ein klarer Zeitplan, strukturierte Abarbeitung. Viele Quick-Wins lassen sich in einer konzentrierten 6-Wochen-Phase schließen.

Cluster 3: Umgang mit Sicherheitsvorfällen

> **Was in diesem Cluster liegt:** Alle Findings zur Erkennung von Vorfällen, zur Klassifikation, zur Meldung an die BaFin und zum internen Eskalationsprozess.

Typische Findings

- Klassifikations-Matrix existiert, ist aber nicht aktuell
- Meldeprozess an die BaFin wurde nicht innerhalb der letzten 12 Monate geprobt
- Angriffserkennungs-Regeln sind länger als 18 Monate alt
- Eskalations-Kette dokumentiert, aber Verantwortliche nicht mehr im Unternehmen
- Dokumentation der letzten Fälle lückenhaft

Zeitaufwand und Komplexität

Dimension	Einordnung
Zeitaufwand	Mittel (4 bis 10 Wochen)
Komplexität	Mittel bis hoch (berührt IT, Compliance und Geschäftsleitung)
Quick-Wins möglich?	Teilweise (z. B. Klassifikations-Matrix aktualisieren)
Langläufer?	Der Probe-Prozess und die Dokumentation

Der typische Fallstrick

Der Meldeprozess an die BaFin ist ein Dokument, das auf Papier existiert. Der Wirtschaftsprüfer will aber den Beleg einer Probe. Eine Probe durchzuführen heißt: Kalender koordinieren, Szenario entwickeln, Teilnehmer einladen, auswerten, dokumentieren. Das dauert realistisch 6 bis 8 Wochen.

Was wir in der Praxis empfehlen: Die Probe ist planbar und sollte früh terminiert werden. Der Rest des Clusters läuft parallel. Wichtig: Die Verantwortlichen für die Meldewege müssen aktuell sein, nicht nur namentlich im Dokument stehen.

Cluster 4: Notfallplanung

> **Was in diesem Cluster liegt:** Alle Findings zur Aufrechterhaltung des Geschäftsbetriebs bei Ausfällen. Von den Wiederanlaufzeiten bis zu den praktischen Übungen.

Typische Findings

- Notfallpläne existieren, aber Wiederanlauf-Tests länger als 12 Monate zurück
- Maximal tolerierbare Ausfallzeiten theoretisch definiert, aber nicht validiert
- Mindestversorgungsniveaus fehlen für wichtige Funktionen
- Kommunikations-Pläne für den Krisenfall veraltet
- Redundanzen technisch vorhanden, aber nicht unter realistischen Bedingungen getestet

Zeitaufwand und Komplexität

Dimension	Einordnung
Zeitaufwand	Hoch (8 bis 20 Wochen)
Komplexität	Sehr hoch (berührt IT, Fachbereiche, Geschäftsleitung)
Quick-Wins möglich?	Selten
Langläufer?	Fast immer

Der typische Fallstrick

Wiederanlauf-Tests sind der schwierigste Teil jeder Nacharbeit. Sie brauchen Vorbereitung, sie unterbrechen den Betrieb, sie erfordern Abstimmung mit mehreren Bereichen. Viele Institute legen das Thema an, schieben aber die praktische Durchführung. Der nächste Prüfer sieht das sofort.

Was wir in der Praxis empfehlen: Dieser Cluster gehört in die erste Prioritätsgruppe, aber nicht in die Schnellbearbeitung. Realistische Planung über 4 bis 6 Monate, mit externer Projektleitung. Wer hier strukturell aufräumt, hat für die nächsten drei Prüfzyklen Ruhe.

Cluster 5: Drittparteien-Steuerung

> **Was in diesem Cluster liegt:** Alle Findings zu Ihren IT-Dienstleistern, deren Unter-Dienstleistern, Verträgen und Ausstiegs-Strategien.

Typische Findings

- Register der IT-Dienstleister unvollständig
- Kritikalitäts-Bewertung länger als 18 Monate nicht aktualisiert
- Unter-Dienstleister nicht bis zur zweiten Ebene bekannt
- DORA-Pflichtklauseln fehlen in bestehenden Verträgen
- Ausstiegs-Strategien existieren als Absichtserklärung ohne konkreten Ablauf

Zeitaufwand und Komplexität

Dimension	Einordnung
Zeitaufwand	Sehr hoch (12 bis 30 Wochen)
Komplexität	Sehr hoch (erfordert Nachverhandlungen, externe Kooperation)
Quick-Wins möglich?	Nur bei Register-Pflege
Langläufer?	Ja, fast alle Findings hier

Der typische Fallstrick

Vertragliche Nachverhandlungen mit Cloud-Anbietern und IT-Dienstleistern sind zeitintensiv. Viele Dienstleister wehren sich gegen neue Klauseln oder verlangen Preisanpassungen. Wer das unterschätzt, hat Ende des Jahres einen neuen Prüfbericht mit den gleichen Findings.

Was wir in der Praxis empfehlen: Dieser Cluster ist der größte Hebel der DORA-Compliance und gleichzeitig der risikoreichste. Wir empfehlen, hier frühzeitig externe Unterstützung zu holen, die in der Branche vernetzt ist und die Vertragsverhandlungen effizient moderieren kann.

Cluster 6: Dokumentation und Nachweise

> **Was in diesem Cluster liegt:** Alle Findings zu Richtlinien, Arbeitsanweisungen, Protokollen und Nachweisen, die formal vorliegen müssen.

Typische Findings

- Richtlinien länger als 12 Monate nicht aktualisiert
- Aktualisierungs-Historie in Dokumenten lückenhaft
- Freigaben durch die Geschäftsleitung nicht nachvollziehbar dokumentiert
- Verknüpfung zwischen Richtlinien und operativer Umsetzung fehlt
- Nachweise für Schulungen, Prüfungen und Vorfälle unvollständig

Zeitaufwand und Komplexität

Dimension	Einordnung
Zeitaufwand	Niedrig (1 bis 4 Wochen pro Dokument)
Komplexität	Niedrig (Einzelarbeit, wenig Abstimmung nötig)
Quick-Wins möglich?	Ja, nahezu alle Findings hier
Langläufer?	Nur bei großen Dokumentations-Lücken

Der typische Fallstrick

Dokumentations-Findings wirken trivial und werden oft vernachlässigt. Der Denkfehler: „Das machen wir nebenher." Das Ergebnis ist, dass zum Ende des Prüfzyklus immer noch 15 bis 20 Dokumentations-Findings offen sind, weil sie nie Priorität hatten.

Was wir in der Praxis empfehlen: Dieser Cluster ist der perfekte Anfang. Wer hier in der ersten Woche 5 bis 10 Findings schließt, hat schnelle Erfolge für das Team, zeigt Fortschritt gegenüber dem Vorstand und schafft Momentum für die schwereren Cluster.

Die Bewertungs-Matrix: Zeitaufwand und Komplexität

Jedes Finding lässt sich in zwei Dimensionen bewerten: Zeitaufwand und Komplexität. Die Matrix hilft, aus der Findings-Liste eine belastbare Priorisierung zu machen.

Die 2×2-Matrix

	Niedrige Komplexität	**Hohe Komplexität**
Kurzer Zeitaufwand	**Quick-Wins** sofort abarbeiten	**Schnelle Projekte** gut vorbereiten
Langer Zeitaufwand	**Sortieren** in der Pipeline halten	**Langläufer** Projekt-Status geben

Was in welches Feld fällt

Quick-Wins (Woche 1 bis 4):

- Cluster 6: Dokumentations-Findings
- Einzelne Cluster-2-Findings (z. B. MFA-Einführung für klare Nutzergruppen)
- Cluster 3: Klassifikations-Matrix-Aktualisierung

Schnelle Projekte (Woche 2 bis 8):

- Cluster 3: Probe-Prozess für BaFin-Meldung
- Cluster 2: Berechtigungsrevision

Sortieren (läuft im Hintergrund):

- Cluster 5: Register-Pflege und Unter-Dienstleister-Erfassung

Langläufer (Monat 2 bis 6):

- Cluster 1: Risiko-Rahmenwerk-Überarbeitung
- Cluster 4: Wiederanlauf-Tests und BCM-Struktur
- Cluster 5: Vertragsverhandlungen

Die Realität

Typische Nacharbeit für 80 bis 100 Findings verteilt sich so:

Kategorie	Anteil	Dauer bis Abschluss
Quick-Wins	30 bis 40 %	4 bis 6 Wochen
Schnelle Projekte	15 bis 20 %	8 bis 12 Wochen
Sortieren	10 bis 15 %	laufend
Langläufer	30 bis 40 %	4 bis 6 Monate

Das bedeutet: Wer realistisch plant, braucht für die strukturelle Abarbeitung 5 bis 7 Monate. Wer das unterschätzt und in 8 Wochen fertig sein will, landet im nächsten Prüfzyklus mit halber Nacharbeit.

Der Hebel der strukturierten Herangehensweise: Sie reduziert die Gesamtzeit nicht um 50 Prozent. Sie reduziert die Zahl der Findings, die nach einem Jahr noch offen sind, von typischerweise 15 bis 25 auf unter 5.

Vorlage Findings-Tracking + Nächste Schritte

Vorlage: Findings-Tracking (direkt einsatzbereit)

Die folgende Struktur können Sie direkt in Excel oder Ihrer Projekt-Management-Software übernehmen.

Spalte	Inhalt
Finding-ID	Interne Nummer oder Nummer aus dem Prüfbericht
Kurzbeschreibung	1 Satz, klar und verständlich
Cluster	1 bis 6 (aus diesem Dokument)
Zeitaufwand	Kurz / Lang
Komplexität	Niedrig / Hoch
Matrix-Feld	Quick-Win / Schnelles Projekt / Sortieren / Langläufer
Verantwortlich	Name + Fachbereich
Startdatum	Geplanter Beginn
Zieldatum	Geplanter Abschluss
Nachweis	Link zum Dokument oder Speicher-Ort
Status	Offen / In Arbeit / Abgeschlossen / Verschoben

Diese Struktur erfüllt drei Anforderungen: Sie ist einfach genug, dass jedes Team sie anwenden kann. Sie ist vollständig genug, um dem Prüfer die Nacharbeit zu belegen. Sie ist filterbar genug, um auf Vorstands-Ebene zu reporten.

Ihr nächster Schritt

Sie haben jetzt das Framework. Sie kennen die 6 Cluster. Sie haben die Bewertungs-Matrix. Sie haben die Tracking-Vorlage.

Die ehrliche Frage: Reicht das, um 80 oder 300 Findings strukturiert abzuarbeiten?

In den meisten Fällen nicht. Nicht weil das Framework unvollständig ist, sondern weil die Nacharbeit selbst komplex ist. Vertragsverhandlungen mit Cloud-Anbietern brauchen Branchen-Kontakte. Wiederanlauf-Tests brauchen Erfahrung mit realistischen Szenarien. Risiko-Rahmenwerke brauchen einen Blick von außen, damit sie nicht die Fehler der vorherigen Version wiederholen.

Unser Angebot: Kostenlose Potenzialanalyse

In einem 30-minütigen Gespräch schauen wir gemeinsam auf Ihre konkrete Findings-Liste. Wir clustern sie mit Ihnen durch. Wir bewerten Zeitaufwand und Komplexität. Wir machen Ihnen einen konkreten Vorschlag für die nächsten 8 Wochen.

Kein Pitch. Kein Druck. Eine ehrliche Einschätzung.

→ **Kostenlose Potenzialanalyse buchen** *[Link in der E-Mail, die Sie erhalten haben]*

Über Bennert Consulting

Bennert Consulting begleitet Banken, Versicherungen und Leasinggesellschaften durch DORA-Prüfungen und die strukturierte Nacharbeit danach.

Unsere aktuellen Mandate:

- Versicherer, laufende Nacharbeit aus erster Prüfung: LKH
- DAX-Konzern, DORA vollständig umgesetzt:Mercedes Benz Leasinggesellschaft, LKH, VWD Transaction Solutions AG

Was uns auszeichnet: Keine Nebelkerzen. Keine 80-Seiten-Theorie. Direkte Umsetzung mit Vorlagen, die der Prüfer akzeptiert.

Kontakt

Bennert Consulting
Marc Bennert
marc@bennert-consulting.de | +49 175 41 65 823
bennertconsulting.de

Dieses Dokument ist eine allgemeine Orientierungshilfe zur Nacharbeit nach der DORA-Prüfung. Es ersetzt keine individuelle Beratung. Rechtliche Bewertungen müssen im Einzelfall durch qualifizierte Fachkräfte erfolgen.