

Verhältnismäßigkeit unter DORA und MaRisk

Vom Mindeststandard zum begründeten und prüfbaren Zielreifegrad

LEITTHESE Verbandsstandards und Baselines sind der Ausgangspunkt, nicht automatisch das angemessene Zielbild. Verhältnismäßigkeit entsteht aus dem institutsindividuellen Profil und dem Nachweis wirksamer Steuerung.

1 Verhältnismäßigkeitsprofil nach Art. 4 DORA

1 Größe

20 %

Bilanzsummenband, Reichweite, Geschäftsstruktur und operative Wirkung.

2 Gesamtrisikoprofil

35 %

IKT-Risiko, Restrisiko, Bedrohung, Vorfälle, Feststellungen und Risikotoleranz.

3 Art und Umfang

20 %

Leistungsbreite, Volumen, digitale Kanäle, Zeitkritikalität und Kundenwirkung.

4 Komplexität

25 %

Architektur, Schnittstellen, Legacy, Drittparteien, Gruppen- und Cloud-Abhängigkeiten.

PROFILWERT $0,20 \times \text{Größe} + 0,35 \times \text{Risikoprofil} + 0,20 \times \text{Art und Umfang} + 0,25 \times \text{Komplexität}$
Score unterstützt die Entscheidung. Fachliche Beurteilung und Mindestniveaus haben Vorrang.

2 Begründungskette in acht Schritten

1 Rechtsrahmen abgrenzen

DORA-Kategorie, MaRisk-Anwendung, Gruppenebene und Bilanzbasis festlegen.

2 Baseline bestimmen

Zwingende Anforderungen und ausdrücklich eröffnete Erleichterungen dokumentieren.

3 Evidenz erheben

Risikoinventur, BIA, Register, Vorfälle, Tests, Architektur und Kennzahlen zusammenführen.

4 Profil bewerten

Vier Faktoren auf einer Skala von 1 bis 5 nachvollziehbar einstufen.

5 Risikoverstärker anwenden

Kritische Funktionen, Schadenspotenzial und Konzentrationen als Mindestniveau berücksichtigen.

6 Zielreife festlegen

Profilklasse, Eskalationsregeln und Managementbeurteilung zusammenführen.

7 Ist-Reife und Lücke messen

Design, Umsetzung und Wirksamkeit je Domäne anhand belastbarer Nachweise bewerten.

8 Entscheiden und überwachen

Zielbild, Maßnahmen, Restrisiko, Verantwortliche und Aktualisierung genehmigen.

METHODISCHES ERGEBNIS

Profilklasse + Zielreifegrad + Domänenziele + Reifegradlücken + genehmigter Maßnahmenplan + Wirksamkeitsnachweis

Vom Profil zum prüfbaren Zielbild

Der Zielreifegrad folgt aus Risiko und Wirkung, nicht aus dem vorhandenen Umsetzungsstand

3 Fünfstufiges Reifegradmodell

1	Mindeststandard	Baseline und generische Ausgestaltung	E1 Konzept
2	Definiert	Profil, Methodik, Rollen und Zielbild	E1 plus Beschluss
3	Implementiert	Organisatorisch und technisch umgesetzt	mindestens E2
4	Gesteuert	Kennzahlen, Tests, Audits und Management	mindestens E3
5	Optimiert und resilient	Dynamische Kalibrierung und Automatisierung	mindestens E4

ZIELKORRIDOR

P1 und P2: RG 3 | P3: RG 3, kritische Domänen RG 4 | P4: RG 4 | P5: RG 4, hochkritische Domänen RG 5

4 Eskalationsregeln verhindern Scheingenaugkeit

- Gesetzliche Mindestanforderungen und domänenspezifische Mindestniveaus sind nicht verrechenbar.
- Zwei Kernfaktoren mit Wert 4 oder 5 führen grundsätzlich zu einem Zielreifegrad von mindestens 4.
- Kritische Funktionen, hohe Schadenswirkung oder fehlende Substituierbarkeit erhöhen betroffene Domänen.
- Schwerwiegende Vorfälle und Feststellungen senken den Ist-Reifegrad, nicht das erforderliche Ziel.
- Gesamtreife folgt bei kritischen Domänen dem Prinzip des schwächsten Glieds.

GOVERNANCE UND FREIGABE

- Bilanzbasis, Meldekreis, Verbund-, Holding- und Konsolidierungseffekte festlegen.
- Schwellenwerte durch Risikomanagement und Leitungsorgan genehmigen.
- Institutsstichprobe jährlich aktualisieren und Nutzung förmlich freigeben.
- 5 Mrd. Euro: interner Reifegradtrigger, keine automatische EZB-Einstufung.

BERECHNUNGSTOOL

- Strukturierte Erfassung der vier Faktoren mit Evidenzbezug.
- Automatische Profilkategorie und Vorschlag für den Zielreifegrad.
- Domänenziele, Ist-Reifegrade, Lücken und Maßnahmensteuerung.
- Management-Dashboard und integrierte Anwendungshinweise.

Berechnungstool mit ausführlicher Methodik

Das Berechnungstool sowie die ausführliche Methodik können beim Sachverständigenbüro Schulte bezogen werden.

itschulte.de/kontakt

Fachlicher Standardvorschlag zur internen Operationalisierung