Provider-Risikobewertung — Template

Version 1.0 | Mai 2026 | Alexander Martens

---

1. Bewertungsmethodik

Die Risikobewertung erfolgt in zwei Stufen:

1. **Inhärentes Risiko** — Risiko vor Berücksichtigung von Kontrollen
2. **Residualrisiko** — Verbleibendes Risiko nach Kontrollen

Formel: Residualrisiko = Inhärentes Risiko × (1 − Kontrollreife)

---

2. Inhärentes Risiko (1–5)

Kriterium	Gewicht	Score (1–5)	Gewichtet
Kritikalität der Dienstleistung	30 %		
Umfang des Datenzugriffs	25 %		
Substituierbarkeit (1 = einfach, 5 = unmöglich)	20 %		
Geografisches / politisches Risiko	15 %		
Reputationsrisiko bei Ausfall	10 %		
Inhärentes Risiko (gewichtet)	**100 %**		

Bewertungsskala:

- 1.0–2.0: Niedrig
- 2.1–3.5: Mittel
- 3.6–5.0: Hoch

---

3. Kontrollreife (0–100 %)

Kontrollbereich	Gewicht	Reifegrad (0–100 %)	Gewichtet
Zertifizierungen (ISO 27001, SOC2, C5, BSI	25 %		

Kontrollbereich	Gewicht	Reifegrad (0–100 %)	Gewichtet
IT-Grundschutz)			
Vertragliche Sicherheitsmaßnahmen (Art. 28 Abs. 7)	20 %		
SLA-Reporting und Transparenz	15 %		
Incident-Historie (letzte 24 Monate)	15 %		
Exit-Readiness (getestet?)	15 %		
Subunternehmer-Transparenz	10 %		
Kontrollreife (gewichtet)	**100 %**		

---

4. Residualrisiko-Berechnung

	Wert
Inhärentes Risiko	
Kontrollreife	%
Residualrisiko = Inhärent × (1 − Reife)	

---

5. Bewertungsbogen

Dienstleister: _____

Datum der Bewertung: _____

Bewertet durch: _____

Kriterium Inhärentes Risiko	Score (1–5)	Begründung
Kritikalität		
Datenzugriff		
Substituierbarkeit		
Geografisches Risiko		
Reputationsrisiko		

Kontrollbereich	Reifegrad (0–100 %)	Nachweis
Zertifizierungen		
Vertragliche Sicherheit		
SLA-Reporting		
Incident-Historie		
Exit-Readiness		
Subunternehmer		

Ergebnis:

- Inhärentes Risiko: ___ (niedrig/mittel/hoch)
- Kontrollreife: ___ %
- Residualrisiko: ___ (niedrig/mittel/hoch)
- Handlungsbedarf: ☐ keiner ☐ Maßnahmen einleiten ☐ Eskalation

---

Disclaimer: Dieses Template ist ein Vorschlag zur institutsspezifischen Anpassung.