

LIEFERANTENBEWERTUNGSMATRIX

TPRM-TRIAGE NACH ISO 27001, NIS2 UND DORA

TEIL 1 KRITIKALITÄTSEBEWERTUNG – bestimmt den Tier

Bewertung 1 bis 3 Punkte je Dimension, Summe ergibt Tier-Zuordnung

DATENZUGANG

Greift der Lieferant auf Daten zu?



- 3** Zugang zu personenbezogenen, vertraulichen oder betriebskritischen Daten. Verarbeitung im Auftrag oder Speicherung beim Lieferanten.
- 2** Indirekter Zugang, z. B. über gemeinsam genutzte Systeme oder Support-Zugänge. Kein aktiver Datentransfer.
- 1** Kein Datenzugang. Rein physische oder nicht-digitale Lieferbeziehung.

SYSTEMZUGANG

Hat der Lieferant IT-Zugang?



- 3** Direkter, regelmäßiger Zugang zu internen IT-Systemen, Netzwerken oder Produktionssystemen (z. B. Remote-Wartung, VPN, API-Integration).
- 2** Gelegentlicher oder eingeschränkter Systemzugang. Nur auf Anfrage oder zeitlich begrenzt.
- 1** Kein Systemzugang. Keine digitale Schnittstelle zum eigenen Betrieb.

BETRIEBSRELEVANZ

Wirkung bei 30-tägigem Ausfall?



- 3** Ausfall beeinträchtigt den Geschäftsbetrieb innerhalb von 72 Stunden erheblich oder bringt ihn zum Stillstand. Kein kurzfristiger Ersatz verfügbar.
- 2** Ausfall beeinträchtigt den Betrieb, aber Workarounds oder Teilersatz sind innerhalb von 1-4 Wochen möglich.
- 1** Ausfall hat keine wesentliche Betriebsauswirkung. Sofortiger Ersatz verfügbar oder Lieferung nicht zeitkritisch.

REGULATORISCHE RELEVANZ

NIS2 / DORA / CRA / DSGVO



- 3** Lieferant berührt direkt regulatorische Pflichtbereiche: NIS2-Lieferkettenpflichten, DORA IKT-Drittanbieter, CRA-relevante Software, DSGVO-Auftragsverarbeitung.
- 2** Indirekte regulatorische Berührung. Lieferant liefert in regulierte Bereiche, ohne selbst direkt in Scope zu fallen. Dokumentation empfohlen.
- 1** Keine erkennbare regulatorische Relevanz. Außerhalb regulierter Bereiche und ohne Datenschutzrelevanz.

SUBSTITUIERBARKEIT

Wie schnell ersetzbar?



- 3** Schwer oder nicht kurzfristig substituierbar. Wechsel dauert mehr als 3 Monate oder verursacht erhebliche Kosten. Kein qualifizierter Alternativanbieter bekannt.
- 2** Substituierbar innerhalb 1-3 Monaten. Alternativanbieter bekannt, aber Wechsel aufwendig.
- 1** Leicht substituierbar. Mehrere Alternativanbieter verfügbar, Wechsel innerhalb von Wochen möglich.



TIER-ZUORDNUNG

TIER A – KRITISCH

Score 13–15 Punkte



Vollständige Prüfung, individuelle Vertragsgestaltung, laufendes Monitoring.

TIER B – RELEVANT

Score 8–12 Punkte



Standardisiertes Assessment oder Zertifikatsnachweis. Jährliche Überprüfung.

TIER C – UNKRITISCH

Score ≤ 7 Punkte



Selbstauskunft oder Basischeck. Anlassbezogene Prüfung, kein regelmäßiges Audit.

TEIL 2 AUDIT-LEVEL UND PRÜFMAßNAHMEN JE TIER

	TIER A – KRITISCH	TIER B – RELEVANT	TIER C – UNKRITISCH
PRÜFFORMAT	Vollständiges TPRM-Assessment: adaptierter Fragebogen (CAIQ, SIG oder eigenentwickelt), ggf. Vor-Ort-Gespräch oder Remote-Interview.	Standardisierter Kurzfragebogen (max. 15–20 Fragen) oder Nachweis einer anerkannten Zertifizierung (ISO 27001, SOC 2, TISAX).	Fünf-Fragen-Selbstauskunft, anlassbezogen. Keine regelmäßige Prüfung erforderlich.
AKZEPTIERTER NACHWEIS	ISO-27001-Zertifikat + Ergänzungsfragen zu Vorfallmeldung, Subdienstleistern, Ausstiegsplanung. Oder: vollständiger Fragebogen mit Plausibilisierung.	ISO-27001-, SOC-2- oder TISAX-Zertifikat ohne Ergänzungsfragen. Oder: Kurzfragebogen ohne Vor-Ort-Verifizierung.	Selbstauskunft ohne unabhängigen Nachweis ausreichend. Bei Auffälligkeiten: Eskalation zu Tier B.
PRÜFFREQUENZ	Jährliches Vollassessment + kontinuierliches Monitoring (SecurityScorecard, BitSight o. ä.). Ereignisbasierte Nachprüfung bei Score-Verschlechterung > 15 %.	Jährlicher Kurzfragebogen oder Zertifikatserneuerungsnachweis. Monitoring empfohlen, aber nicht verpflichtend.	Einmalige Ersterfassung. Wiederholung bei Vertragsänderung oder auf Anlass. Kein regelmäßiges Monitoring.
VERTRAGLICHE MINDESTANFORDERUNGEN	Auditklausel, Meldepflicht bei Sicherheitsvorfällen (max. 24 h), Subdienstleister-Offenlegungspflicht, Exit-Klausel mit Datenlösch-Regel, SLA mit messbaren Sicherheits-KPIs.	Meldepflicht bei Sicherheitsvorfällen, Datenschutz-Grundvereinbarung (AV-Vertrag wenn relevant). Auditklausel empfohlen.	Standardlieferantenvertrag mit DSGVO-Grundklausel. Keine Sonderpflichten.
ZUSTÄNDIGKEIT INTERN	Einkauf + IT-Sicherheit + ggf. Recht. Abnahme durch CISO oder ISB erforderlich.	Einkauf mit IT-Kurzcheck. Keine CISO-Abnahme erforderlich.	Einkauf allein. Kein IT-Involvement erforderlich.

AUF EINEN BLICK



1. BEWERTEN
5 Dimensionen bewerten (1–3 Punkte)



2. TIER BESTIMMEN
Summe bildet Tier A, B oder C



3. PRÜFEN
Passendes Audit-Level und Nachweise durchführen



4. ÜBERWACHEN
Monitoring entsprechend Tier-Level



5. REAGIEREN
Eskalationslogik bei Änderungen oder Vorfällen

TEIL 3 HANDLUNGSEMPFEHLUNGEN UND ESKALATIONSLOGIK

	TIER A – KRITISCH	TIER B – RELEVANT	TIER C – UNKRITISCH
LIEFERANT VERWEIGERT AUSKUNFT	Risiko dokumentieren, alternative Anbieter qualifizieren, Vertragsverlängerung von Nachbesserung abhängig machen.	Nachfassen; bei weiterer Verweigerung zu Tier A hochstufen.	Selbstauskunft als nicht erbracht dokumentieren. Kein weiterer Handlungsbedarf bei weiterhin niedriger Kritikalität.
LIEFERANT HAT KEINE ZERTIFIZIERUNG	Fragebogen-basierte Vollprüfung verpflichtend. Zertifizierung als mittelfristiges Vertragsziel definieren (z. B. binnen 18 Monaten).	Fragebogen-Prüfung ausreichend. Zertifizierung empfehlen, nicht erzwingen.	Keine Anforderung an Zertifizierung.
SCORE-VERSCHLECHTERUNG IM MONITORING	Ab -15 %: Proaktiver Kontakt, Klärung der Ursache. Ab -30 %: Formelle Nachprüfung, ggf. Eskalation zu Krisenprotokoll.	Bei starker Verschlechterung: zu Tier A hochstufen und entsprechend verfahren.	Kein Monitoring vorgesehen.
SICHERHEITSVORFALL BEIM LIEFERANTEN	Sofortige Kontaktaufnahme, Schadensausmaß klären, eigene Systeme auf Kompromittierung prüfen, Meldepflichten nach NIS2/DORA prüfen.	Kontaktaufnahme und Risikoabschätzung. Ggf. zu Tier A hochstufen.	Information abwarten, bei Relevanz nachfassen.
VERTRAGSVERLÄNGERUNG ANSTEHT	Aktuelle Bewertung als Verlängerungsvoraussetzung. Neue Vertragsklauseln (Audit, Meldung, Exit)	Zertifikatsnachweis als Verlängerungsvoraussetzung.	Standarderneuerung ohne Sonderbedingungen.