IKT-DRITTPARTEIENRISIKO

Vereinbart ist nicht gelebt.
12 Fragen für Ihre Dienstleisterprüfung nach DORA.

Die meisten IKT-Dienstleisterverträge erfüllen auf dem Papier die Anforderungen der DORA. Ob die Vorgaben im Alltag des Dienstleisters tatsächlich umgesetzt werden, zeigt erst der Nachweis. Diese Fragen helfen Ihnen, genau das zu prüfen – mit konkreten Belegen statt Selbstauskünften.

Auswählen
Für jeden Dienstleister 4–6 Fragen, die zum Risiko der unterstützten Funktion passen. Bei kritischen oder wichtigen Funktionen alle Fragen.

Nachweis verlangen
Stichproben aus echten Tickets, Reports und Protokollen – nicht nur Richtlinien, Zertifikate oder Präsentationen.

Dokumentieren
Ergebnis, Abweichung und vereinbarte Maßnahme festhalten – und bei der nächsten Prüfung die Wirksamkeit nachverfolgen.

01 Kennt der Dienstleister Ihre Sicherheitsvorgaben – oder nur den Vertrag?

NACHWEIS VERLANGEN
Die operativ Verantwortlichen beim Dienstleister können die für Sie geltenden Vorgaben benennen; sie sind in dessen Prozesse, Arbeitsanweisungen und Tickets übernommen.

WARNSIGNAL
Als Antwort kommt nur der Verweis auf die eigene ISO-27001-Zertifizierung oder allgemeine Konzernrichtlinien.

Bezug: Art. 30 Abs. 2 lit. c, Abs. 3 lit. c* DORA

02 Werden IKT-Vorfälle innerhalb der vereinbarten Fristen gemeldet – nachweisbar?

NACHWEIS VERLANGEN
Stichprobe von Vorfällen der letzten 12 Monate: Zeitpunkt der Erkennung, der Meldung an Sie und der Unterstützung bei der Bearbeitung.

WARNSIGNAL
Keine einzige Meldung in 12 Monaten – oder Meldungen erst, nachdem Sie selbst nachgefragt haben.

Bezug: Art. 30 Abs. 2 lit. f, Abs. 3 lit. b* DORA · Ihre eigene Meldepflicht: Art. 19 DORA

03 Sind die Service Levels messbar – und werden sie tatsächlich gemessen?

NACHWEIS VERLANGEN
Regelmäßige Reports mit Ist-Werten gegen die vereinbarten Ziele; bei Abweichungen die eingeleiteten Korrekturmaßnahmen.

WARNSIGNAL
Reports zeigen nur „grün", ohne Messwerte – oder die Kennzahlen wurden seit Vertragsbeginn nie angepasst.

Bezug: Art. 30 Abs. 2 lit. e, Abs. 3 lit. a* DORA

04 Werden Schwachstellen in Ihren Systemen innerhalb der vereinbarten Fristen geschlossen?

NACHWEIS VERLANGEN
Aktueller Schwachstellenreport für Ihre Umgebung: Alter offener kritischer Findings, Ausnahmen mit dokumentierter Risikoakzeptanz.

WARNSIGNAL
Kritische Schwachstellen sind älter als die vereinbarte Frist und niemand hat eine Ausnahme genehmigt.

Bezug: Art. 30 Abs. 2 lit. c, Abs. 3 lit. c* DORA

05 Wer hat Zugriff auf Ihre Daten und Systeme – und wird das regelmäßig überprüft?

NACHWEIS VERLANGEN
Aktuelle Liste der Berechtigten inklusive privilegierter Konten, Nachweis der letzten Rezertifizierung, Protokollierung privilegierter Zugriffe.

WARNSIGNAL
Ausgeschiedene Mitarbeitende haben noch Zugänge – oder Sammelkonten ohne persönliche Zuordnung.

Bezug: Art. 30 Abs. 2 lit. c DORA

06 Sind alle Unterauftragnehmer bekannt – und war deren Einsatz zulässig?

NACHWEIS VERLANGEN

Aktuelle Liste der Unterauftragnehmer mit Leistung und Standort, abgeglichen mit Vertrag und Ihrem Informationsregister.

Bezug: Art. 30 Abs. 2 lit. a, Art. 28 Abs. 3 (Informationsregister) DORA

WARNSIGNAL

„Das regelt unser Konzern" – oder die Liste weicht vom Informationsregister ab.

07 Wo werden Ihre Daten tatsächlich verarbeitet und gespeichert – inklusive Backups?

NACHWEIS VERLANGEN

Dokumentierte Standorte (Regionen/Länder) für Betrieb, Speicherung und Backup; Nachweis, dass Sie Änderungen vorab mitgeteilt bekommen haben.

Bezug: Art. 30 Abs. 2 lit. b DORA

WARNSIGNAL

Backups oder Supportzugriffe aus Ländern, die im Vertrag nicht vorkommen.

08 Werden Notfall- und Wiederanlaufpläne getestet – mit Ergebnis?

NACHWEIS VERLANGEN

Protokoll des letzten Tests: Szenario, tatsächlich erreichte Wiederanlaufzeit und Datenverlust gegen die Vorgaben, abgeleitete Maßnahmen.

Bezug: Art. 30 Abs. 3 lit. c* DORA

WARNSIGNAL

Der Plan existiert, wurde aber nie getestet – oder nur als „Tabletop" ohne technischen Wiederanlauf.

09 Werden Ihre Prüf- und Zugangsrechte in der Praxis gewährt?

NACHWEIS VERLANGEN

Ihre letzte eigene Prüfung beim Dienstleister: angeforderte Unterlagen vollständig und fristgerecht erhalten, Vor-Ort-Termin möglich.

Bezug: Art. 30 Abs. 3 lit. e* DORA · risikobasierte Prüfhäufigkeit: Art. 28 Abs. 6 DORA

WARNSIGNAL

Statt Prüfung werden nur Zertifikate oder ein Standard-Prüfbericht angeboten, Detailfragen bleiben unbeantwortet.

10 Werden Findings aus früheren Prüfungen tatsächlich behoben?

NACHWEIS VERLANGEN

Maßnahmenliste mit Status und Termin; für geschlossene Punkte ein Beleg der Wirksamkeit, nicht nur „erledigt".

Bezug: Art. 28 Abs. 6 DORA (Prüfung und Überwachung des Dienstleisters)

WARNSIGNAL

Dieselben Findings tauchen Jahr für Jahr wieder auf – mit neuem Zieltermin.

11 Ist der Dienstleister in Ihre Awareness-Programme und Tests eingebunden?

NACHWEIS VERLANGEN

Teilnahmenachweise an Ihren Sensibilisierungs- und Resilienzschulungen; bei kritischen Funktionen die Mitwirkung an TLPT.

Bezug: Art. 30 Abs. 2 lit. i, Abs. 3 lit. d* DORA

WARNSIGNAL

Die Teilnahme ist vertraglich vereinbart, wurde aber nie eingefordert.

12 Ist der Ausstieg realistisch vorbereitet – inklusive Rückgabe Ihrer Daten?

NACHWEIS VERLANGEN

Dokumentierte Ausstiegsstrategie mit Übergangszeitraum, Datenformat für die Rückgabe und einer Einschätzung, wer die Leistung übernehmen könnte.

Bezug: Art. 28 Abs. 8, Art. 30 Abs. 2 lit. d, Abs. 3 lit. f* DORA

WARNSIGNAL

Die Exit-Strategie ist ein Absatz im Vertrag – niemand weiß, wie lange ein Wechsel tatsächlich dauern würde.

* Anforderungen nach Art. 30 Abs. 3 DORA gelten für vertragliche Vereinbarungen über IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen. Artikelangaben beziehen sich auf die Verordnung (EU) 2022/2554 (DORA).
Diese Checkliste dient der allgemeinen Orientierung. Sie ist keine Rechtsberatung und ersetzt keine Prüfung im Einzelfall.

Sie wollen wissen, wo Ihre Dienstleister wirklich stehen?

Ich unterstütze bei Wirksamkeitsprüfungen kritischer IKT-Dienstleister nach DORA – von der Prüfplanung bis zur Nachverfolgung der Maßnahmen.

alec.fuchs@f-sec.eu
f-sec.eu

© 2026 Fuchs Security · Alec Fuchs, CISSP