Muster-Prüfprogramm

DORA

IKT-Drittparteienrisiko

14 Prüfschritte · DORA

14 Prüfschritte mit Kriterium, Fundstelle, Prüfhandlung und erwarteten Nachweisen. 8 Unterlagen zur Anforderung und die typischen Feststellungen.

DORA Art. 28 Abs. 1 · DORA Art. 28 Abs. 2 · DORA Art. 28 Abs. 3 · DORA Art. 28 Abs. 4 · DORA Art. 28 Abs. 4, Art. 29 · DORA Art. 28 Abs. 5 · DORA Art. 30 Abs. 2 · DORA Art. 30 Abs. 3 · DORA Art. 28 Abs. 6 · Art. 30 Abs. 3 lit. e · DORA Art. 28 Abs. 7 · DORA Art. 28 Abs. 8 · DORA Art. 30 Abs. 3 lit. a und b

Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob das Finanzunternehmen das Risiko aus der Nutzung von IKT-Dienstleistern als Teil seines IKT-Risikomanagements steuert und die Verantwortung für die Einhaltung seiner Pflichten behält. Im Mittelpunkt stehen Strategie, Informationsregister, Auswahl, Vertragsgestaltung, laufende Überwachung und Ausstiegsplanung.

GELTUNGSBEREICH

- Alle vertraglichen Vereinbarungen über IKT-Dienstleistungen, mit Schwerpunkt auf Dienstleistungen für kritische oder wichtige Funktionen
- Einkauf, Vertragsmanagement, Informationssicherheit, Fachbereiche und Leitung als Beteiligte des Prozesses
- Unternehmen im Anwendungsbereich der Verordnung (EU) 2022/2554; die Anwendbarkeit und die Verhältnismäßigkeit klären Sie vorab
- Nicht Gegenstand: die Aufsicht über kritische IKT-Drittdienstleister durch die europäischen Aufsichtsbehörden

Prüfschritte 1 bis 3

Schritt 01 DORA Art. 28 Abs. 1

Die Verantwortung für das Drittparteienrisiko liegt beim Finanzunternehmen und ist Teil des IKT-Risikomanagementrahmens.

Prüfhandlung Rahmenwerk und Zuständigkeiten lesen, Rollen für Steuerung, Überwachung und Eskalation von Dienstleisterbeziehungen feststellen.

Nachweise IKT-Risikomanagementrahmen, Rollenbeschreibungen, Organigramm

Schritt 02 DORA Art. 28 Abs. 2

Eine Strategie für das IKT-Drittparteienrisiko besteht, enthält eine Leitlinie zu Diensten für kritische oder wichtige Funktionen und wird regelmäßig überprüft; das Leitungsorgan überprüft die Risiken aus den Verträgen regelmäßig.

Prüfhandlung Strategie und Leitlinie auf Freigabe, Aktualität und Inhalte prüfen und die Behandlung im Leitungsorgan nachvollziehen.

Nachweise Strategie, Leitlinie, Beschlüsse und Protokolle des Leitungsorgans

Schritt 03 DORA Art. 28 Abs. 3

Ein Informationsregister über alle vertraglichen Vereinbarungen zu IKT-Dienstleistungen wird geführt und ist vollständig.

Prüfhandlung Register mit Vertragsverzeichnis, Kreditorenliste und Einkaufsdaten abgleichen und fehlende Dienstleister ermitteln.

Nachweise Informationsregister, Vertragsverzeichnis, Kreditorenstammdaten

Prüfschritte 4 bis 6

Schritt 04 — DORA Art. 28 Abs. 3

Verträge zu kritischen oder wichtigen Funktionen sind im Register nachvollziehbar gekennzeichnet.

Prüfhandlung Methodik der Einstufung lesen und für eine Stichprobe von Dienstleistungen die Einstufung gegenprüfen.

Nachweise Einstufungsmethodik, Register mit Kennzeichnung, Bewertungsunterlagen

Schritt 05 — DORA Art. 28 Abs. 3

Das Register wird aktuell gehalten, auf Anforderung bereitgestellt und neue oder geänderte Vereinbarungen für kritische Funktionen werden der Aufsicht rechtzeitig gemeldet.

Prüfhandlung Pflegeprozess, letzte Aktualisierung und Meldungen an die Aufsicht ansehen und Fristen mit den Vorgaben abgleichen.

Nachweise Prozessbeschreibung, Änderungshistorie des Registers, Meldungen an die Aufsicht

Schritt 06 — DORA Art. 28 Abs. 4

Vor Vertragsabschluss wird bewertet, ob eine kritische oder wichtige Funktion betroffen ist, welche Risiken bestehen und ob Interessenkonflikte vorliegen.

Prüfhandlung Aus den Verträgen des letzten Jahres eine Stichprobe wählen und die vorvertragliche Bewertung samt Sorgfaltsprüfung durchgehen.

Nachweise Bewertungen vor Vertragsabschluss, Ergebnisse der Sorgfaltsprüfung, Genehmigungen

Prüfschritte 7 bis 10

Schritt 07 — DORA Art. 28 Abs. 4, Art. 29

Konzentrationsrisiken durch einzelne Dienstleister oder durch verbundene Dienstleister werden bewertet.

Prüfhandlung Bewertungsmethodik und letzte Auswertung ansehen und prüfen, ob Abhängigkeiten von einzelnen Anbietern und Standorten erkannt sind.

Nachweise Konzentrationsanalyse, Abhängigkeitsübersicht, Ergebnisse für die Leitung

Schritt 08 — DORA Art. 28 Abs. 5

Verträge werden nur mit Anbietern geschlossen, die angemessene Standards der Informationssicherheit erfüllen.

Prüfhandlung Für eine Stichprobe die Nachweise des Anbieters, etwa Zertifikate oder Prüfberichte, einsehen und die Bewertung dazu prüfen.

Nachweise Zertifikate, Prüfberichte, Bewertung der Nachweise

Schritt 09 — DORA Art. 30 Abs. 2

Verträge enthalten die für alle IKT-Dienstleistungen vorgesehenen Mindestbestandteile.

Prüfhandlung Aus Art. 30 Abs. 2 eine Prüfliste ableiten und eine Stichprobe von Verträgen damit abgleichen.

Nachweise Verträge mit Anlagen, ausgefüllte Prüfliste

Schritt 10 — DORA Art. 30 Abs. 3

Verträge über Dienstleistungen für kritische oder wichtige Funktionen enthalten die zusätzlichen Bestimmungen.

Prüfhandlung Die Stichprobe auf die zusätzlichen Vorgaben für diese Verträge prüfen, darunter Leistungsziele, Notfallpläne und Ausstiegsregelungen.

Nachweise Verträge, Leistungsvereinbarungen, Prüfliste für kritische Funktionen

Prüfschritte 11 bis 14

Schritt 11 — DORA Art. 28 Abs. 6; Art. 30 Abs. 3 lit. e

Zugangs-, Informations- und Prüfrechte sind vereinbart; Häufigkeit und Umfang der Prüfungen beim Anbieter richten sich nach dem Risiko.

Prüfhandlung Prüfplan für Dienstleister ansehen, durchgeführte Prüfungen und Ergebnisse nachvollziehen.

Nachweise Prüfplan für Dienstleister, Berichte, Maßnahmenverfolgung

Schritt 12 — DORA Art. 28 Abs. 7

Kündigungsrechte für die vorgesehenen Fälle sind vertraglich vereinbart und die Ausübung ist organisiert.

Prüfhandlung Kündigungsklauseln in der Stichprobe prüfen und erfragen, wer über die Ausübung entscheidet.

Nachweise Vertragsklauseln, Entscheidungsprozess

Schritt 13 — DORA Art. 28 Abs. 8

Für Dienstleistungen zu kritischen oder wichtigen Funktionen bestehen dokumentierte, getestete und regelmäßig überprüfte Ausstiegsstrategien.

Prüfhandlung Ausstiegspläne lesen, Testnachweise und Übergangspläne für Daten und Dienste prüfen.

Nachweise Ausstiegspläne, Testprotokolle, Übergangskonzepte

Schritt 14 — DORA Art. 30 Abs. 3 lit. a und b

Die Leistung und die Sicherheitsvorfälle bei Dienstleistern werden laufend überwacht und berichtet.

Prüfhandlung Regelberichte und Dienstgüteauswertungen der letzten zwölf Monate ansehen und die Reaktion auf Abweichungen verfolgen.

Nachweise Leistungsberichte, Vorfallmeldungen, Maßnahmenlisten

Unterlagenanforderung

Diese 8 Unterlagen vor Prüfungsbeginn anfordern

1. Strategie und Leitlinie für das IKT-Drittparteienrisiko
2. Informationsregister mit Änderungshistorie
3. Vertragsverzeichnis, Kreditorenliste und Liste der Dienstleister für kritische oder wichtige Funktionen
4. Stichprobe von Verträgen mit Anlagen und Leistungsvereinbarungen
5. Vorvertragliche Bewertungen, Sorgfaltsprüfungen und Konzentrationsanalysen
6. Prüfplan und Prüfberichte zu Dienstleistern
7. Ausstiegspläne mit Testnachweisen
8. Berichte und Beschlüsse des Leitungsorgans zum Thema

TYPISCHE FESTSTELLUNGEN

Das Register ist unvollständig, weil Verträge außerhalb des zentralen Einkaufs geschlossen wurden.

Die Einstufung kritischer oder wichtiger Funktionen ist nicht begründet oder nicht einheitlich.

Vorvertragliche Bewertungen fehlen für bestehende Verträge und wurden bei Verlängerungen nicht nachgeholt.

Bestehende Verträge enthalten nicht alle Mindestbestandteile, etwa zu Unterauftragnehmern oder Datenrückgabe.

Ausstiegspläne bestehen auf dem Papier, wurden aber nie getestet.

Konzentrationsrisiken sind nicht ausgewertet, obwohl mehrere Dienste beim selben Anbieter laufen.

Bibliothek Muster-Prüfprogramme

29 Muster-Prüfprogramme online

proauditmap.com/pruefprogramme/

Vollständiges Prüfpaket in ProAuditMap

proauditmap.com

ProAuditMap

Muster ohne Gewähr und keine Rechtsberatung. Gesetze, Verordnungen und Standards erscheinen nur als Fundstelle, Normtexte sind nicht abgedruckt. Passen Sie Umfang und Tiefe vor der Verwendung an Ihre Organisation, Ihre Risiken und die aktuelle Fassung der für Sie geltenden Vorschriften an. Stand: 13. Oktober 2026