DORA Readiness Checkliste

Systematische Selbstbewertung entlang der fünf DORA-Säulen

Version 1.0 | Mai 2026 | Alexander Martens

Ziel dieser Checkliste

Die DORA Readiness Checkliste übersetzt die 45 Artikel der EU-Verordnung 2022/2554 (Digital Operational Resilience Act) in eine praxisorientierte Selbstbewertung. Sie dient Finanzinstituten als methodische Grundlage für die Standortbestimmung — unabhängig von Größe, Komplexität oder bereits erreichtem Reifegrad.

Abgrenzung: Diese Checkliste versteht sich als Umsetzungshilfe, nicht als abschließendes Prüfschema. Maßgeblich sind die Originalquellen der Aufsicht. Ein negativer Befund in der Selbstbewertung begründet keinen aufsichtsrechtlichen Verstoß, sondern zeigt Handlungsfelder für die weitere DORA-Umsetzung auf.

Anwendungshinweise

Bewertungsschema pro Prüfpunkt:

Status	Bedeutung	Maßnahme
☑ Erfüllt	Anforderung vollständig implementiert und dokumentiert	Regelbetrieb sicherstellen
🟡 In Umsetzung	Maßnahmen eingeleitet, aber noch nicht abgeschlossen	Zeitplan mit Meilensteinen definieren
☐ Offen	Noch nicht begonnen oder keine Dokumentation	Sofortmaßnahme einleiten, Verantwortlichen benennen
☐ N/A	Für das Institut nicht anwendbar (z. B. Opt-out für kleine Institute)	Begründung dokumentieren

Bewertungskontext für kleine und nicht komplexe Institute: Die BaFin hat mit der Aufsichtsmitteilung vom 15. Mai 2026 Erleichterungen für kleine Institute konkretisiert. Prüfpunkte, die ausschließlich für bedeutende Institute gelten, sind mit "(nur bedeutende Institute)" gekennzeichnet.

Säule 1: IKT-Risikomanagement (Art. 5–16)

1.1 Governance und Verantwortung (Art. 5)

Nr	Prüfpunkt	Status	Nachweis / Dokument	Verantwortlich	Frist
1.1.1	Das Leitungsorgan hat die Gesamtverantwortung für das IKT-Risikomanagement übernommen und dies dokumentiert				
1.1.2	Eine IKT-Risikomanagement-Strategie wurde vom Leitungsorgan genehmigt				
1.1.3	Rollen und Verantwortlichkeiten für IKT-Risiken sind definiert und kommuniziert				
1.1.4	Ein IKT-Risikomanagement-Rahmenwerk ist dokumentiert und implementiert				

1.2 Risikoidentifikation und -bewertung (Art. 6–8)

Nr	Prüfpunkt	Status	Nachweis	Verantwortlich	Frist
1.2.1	IKT-Assets sind inventarisiert und klassifiziert (Vertraulichkeit, Integrität,				

Nr	Prüfpunkt	Status	Nachweis	Verantwortlich	Frist
	Verfügbarkeit)				
1.2.2	Ein Prozess zur regelmäßigen Identifikation von IKT-Risiken ist etabliert				
1.2.3	Risikobewertungen werden nach einer definierten Methodik durchgeführt (Eintrittswahrscheinlichkeit × Schadensausmaß)				
1.2.4	Risikoakzeptanzkriterien und Risikotoleranz sind definiert				
1.2.5	Ein IKT-Risikoregister wird geführt und regelmäßig aktualisiert				

1.3 Schutzmaßnahmen und Kontrollen (Art. 9–14)

Nr	Prüfpunkt	Status	Nachweis	Verantwortlich	Frist
1.3.1	Technische und organisatorische Schutzmaßnahmen sind dem Schutzbedarf entsprechend implementiert				
1.3.2	Ein IKT-Kontrollkatalog (z. B. nach ISO 27001 Annex A) ist				

Nr	Prüfpunkt	Status	Nachweis	Verantwortlich	Frist
	definiert und wird regelmäßig auf Wirksamkeit geprüft				
1.3.3	Zugriffsrechte werden nach dem Least-Privilege-Prinzip vergeben und regelmäßig überprüft				
1.3.4	Änderungsmanagement für IKT-Systeme ist etabliert (Test-Freigabe-Produktion)				

1.4 Überwachung und Berichterstattung (Art. 6 Abs. 6–8)

Nr	Prüfpunkt	Status	Nachweis	Verantwortlich	Frist
1.4.1	Key Risk Indicators (KRIs) für IKT-Risiken sind definiert und werden überwacht				
1.4.2	Das Leitungsorgan erhält regelmäßige IKT-Risikoberichte (mindestens jährlich)				
1.4.3	Ein Eskalationsprozess für kritische IKT-Risiken ist definiert				

Säule 2: IKT-Vorfallmanagement (Art. 17–23)

2.1 Vorfallmanagement-Prozess

Nr	Prüfpunkt	Status	Nachweis	Verantwortlich	Frist
2.1.1	Ein IKT-Vorfallmanagement-Prozess ist dokumentiert und implementiert				
2.1.2	Rollen und Verantwortlichkeiten (Incident Response Team) sind definiert				
2.1.3	Ein Klassifizierungsschema für Vorfälle ist etabliert (Major Incident / Significant Incident / Minor)				
2.1.4	Meldewege an die zuständige Aufsichtsbehörde sind definiert und getestet				

2.2 Meldepflichten

Nr	Prüfpunkt	Status	Nachweis	Verantwortlich	Frist
2.2.1	Kriterien für meldepflichtige Vorfälle sind definiert (Art. 18, Art. 19)				

Nr	Prüfpunkt	Status	Nachweis	Verantwortlich	Frist
2.2.2	Meldefristen sind bekannt und im Prozess hinterlegt (Initialmeldung: 4h / Zwischenmeldung: 24h / Abschlussbericht: 1 Monat)				
2.2.3	Ein Melde-Template nach BaFin-Vorgaben ist vorbereitet				
2.2.4	Freiwillige Meldungen an Kunden bei kritischen Vorfällen sind im Prozess vorgesehen				

Säule 3: Digitale operationale Resilienztests (Art. 24–27)

3.1 Testprogramm

Nr	Prüfpunkt	Status	Nachweis	Verantwortlich	Frist
3.1.1	Ein risikobasiertes Testprogramm ist etabliert				
3.1.2	Testarten sind definiert (Art. 25: mindestens 12 Testarten gemäß DORA)				
3.1.3	Testfrequenzen sind risikobasiert festgelegt (Art. 25 Abs. 2: mindestens				

Nr	Prüfpunkt	Status	Nachweis	Verantwortlich	Frist
	jährlich)				
3.1.4	Testergebnisse werden dokumentiert und Maßnahmen abgeleitet				

3.2 TLPT-Pflicht (Art. 26, 27) — nur bedeutende Institute

Nr	Prüfpunkt	Status	Nachweis	Verantwortlich	Frist
3.2.1	TLPT-Pflicht wurde geprüft und dokumentiert				
3.2.2	TLPT-Planung: Frequenz alle 3 Jahre, erstmals bis 17.01.2028				
3.2.3	Externer TLPT-Anbieter identifiziert und beauftragt				

Säule 4: IKT-Drittparteienrisiko (Art. 28–44)

4.1 Informationsregister (Art. 28 Abs. 3)

Nr	Prüfpunkt	Status	Nachweis	Verantwortlich	Frist
4.1.1	Informationsregister aller IKT-Dienstleistungen wird geführt				
4.1.2	Register enthält alle Pflichtfelder nach Art. 28 Abs. 3				

Nr	Prüfpunkt	Status	Nachweis	Verantwortlich	Frist
4.1.3	Register wird laufend aktualisiert und jährlich überprüft				

4.2 Vertragsanforderungen (Art. 28 Abs. 7)

Nr	Prüfpunkt	Status	Nachweis	Verantwortlich	Frist
4.2.1	Alle IKT-Verträge wurden auf DORA-Konformität geprüft				
4.2.2	Exit-Strategien sind für alle kritischen Dienstleister definiert				
4.2.3	Prüfungs- und Zugriffsrechte sind vertraglich vereinbart				

Säule 5: Informationsaustausch (Art. 45)

Nr	Prüfpunkt	Status	Nachweis	Verantwortlich	Frist
5.1	Teilnahme an Informationsaustausch-Arrangements ist geprüft und ggf. umgesetzt				
5.2	Vertraulichkeits- und Datenschutzregelungen für den Austausch sind definiert				

Auswertung

Säule	Max. Punkte	Erreicht	%
1. IKT-Risikomanagement	13		
2. IKT-Vorfallmanagement	8		
3. Resilienztests	7		
4. IKT-Drittparteien	7		
5. Informationsaustausch	2		
Gesamt	**37**		

Handlungsempfehlung:

- 80 %: DORA-Compliance weitgehend erreicht — Fokus auf kontinuierliche Verbesserung
- 50–80 %: Gezielte Maßnahmen in den schwachen Säulen einleiten
- < 50 %: Strukturiertes DORA-Umsetzungsprojekt initiieren
