sosafe

DORA-Compliance-Checkliste

DORA gilt seit dem 17. Januar 2025 und harmonisiert die Vorgaben zur digitalen operationalen Resilienz für Finanzunternehmen in der EU.

Diese Checkliste hilft IT-Verantwortlichen, den eigenen Umsetzungsstand bei DORA strukturiert zu prüfen. Sie ersetzt keine Rechtsberatung und kein formales Prüfverfahren. Sie dient als praxisnahe Vorprüfung für zentrale Themen, die im IT-Betrieb belastbar geregelt, dokumentiert und nachweisbar sein müssen. DORA gilt seit dem 17. Januar 2025 und harmonisiert die Vorgaben zur digitalen operationalen Resilienz für Finanzunternehmen in der EU.

So nutzen Sie diese Checkliste

Prüfen Sie jeden Punkt mit drei Fragen:

- ☑ Ist der Sachverhalt fachlich geregelt?
- ☑ Ist die Umsetzung im Alltag belastbar?
- ☑ Gibt es dafür einen aktuellen Nachweis?

Bewerten Sie jeden Punkt zum Beispiel mit „erfüllt“, „teilweise erfüllt“, „offen“ oder „nicht relevant“. So entsteht schnell ein realistisches Bild über Reifegrad, Lücken und Prioritäten.

1 Executive Governance und Risikosteuerung

Die Geschäftsleitung bleibt unter DORA für Aufsicht und Steuerung verantwortlich. Für Head of IT ist entscheidend, dass Governance, Berichtslinien und Kontrollmechanismen nicht nur definiert, sondern im Betrieb wirksam sind.

CHECKPUNKTE

- [ ] Sind Rollen, Verantwortlichkeiten und Eskalationswege für IKT-Risiken eindeutig festgelegt?
- [ ] Ist dokumentiert, welche Gremien welche Entscheidungen treffen?
- [ ] Erhält die Geschäftsleitung regelmäßig belastbare Berichte zu IKT-Risiken, Vorfällen und Maßnahmen?
- [ ] Sind Risikotoleranzen, Schutzziele und Mindestanforderungen nachvollziehbar festgelegt?
- [ ] Ist klar geregelt, wer Maßnahmen priorisiert, freigibt und nachverfolgt?
- [ ] Sind zentrale Richtlinien aktuell, freigegeben und den zuständigen Teams bekannt?
- [ ] Gibt es einen dokumentierten Prozess, um Kontrollen regelmäßig zu überprüfen und bei Bedarf anzupassen?

NACHWEISE

- Governance-Dokumente und Organigramme
- Risikoberichte und Management-Reports
- Richtlinien, Freigaben und Protokolle
- Kontrollpläne und Review-Termine

2 IKT-Risikomanagement

DORA verlangt ein strukturiertes IKT-Risikomanagement. Risiken müssen identifiziert, bewertet, behandelt und regelmäßig überprüft werden. Das betrifft nicht nur Technik, sondern auch Prozesse, Daten, Abhängigkeiten und Menschen.

CHECKPUNKTE

- [ ] Gibt es ein vollständiges Bild über kritische Systeme, Anwendungen, Datenflüsse und Schnittstellen?
- [ ] Werden IKT-Risiken nach einheitlichen Kriterien bewertet und priorisiert?
- [ ] Sind Risiken mit konkreten Maßnahmen, Fristen und Verantwortlichen verknüpft?
- [ ] Werden Änderungen in der Systemlandschaft in die Risikobewertung übernommen?
- [ ] Sind Notfallvorsorge, Wiederanlauf und Schutzmaßnahmen Teil des Risikomanagements?
- [ ] Werden Risiken regelmäßig neu bewertet, etwa nach Vorfällen, Tests oder wesentlichen Änderungen?
- [ ] Ist nachvollziehbar dokumentiert, welche Restrisiken akzeptiert wurden und von wem?

NACHWEISE

- Risikoinventar und Risikoregister
- Schutzbedarfs- oder Kritikalitätsbewertungen
- Maßnahmenpläne mit Verantwortlichen und Fristen
- Review-Protokolle und Freigaben

3 Incident Reporting und Detection

DORA widmet dem Management, der Klassifizierung und der Meldung IKT-bezogener Vorfälle ein eigenes Kapitel. Für schwere Vorfälle braucht es geregelte Prozesse, klare Zuständigkeiten und harmonisierte Meldungen an die zuständigen Behörden.

CHECKPUNKTE

- ☑ Gibt es einen dokumentierten Prozess zur Erkennung, Bewertung, Eskalation und Bearbeitung von IKT-Vorfällen?
- ☑ Sind Kriterien definiert, nach denen ein Vorfall als schwer eingestuft wird?
- ☑ Wissen IT, Security, Compliance und weitere Fachbereiche, wann sie eingebunden werden müssen?
- ☑ Sind interne und externe Meldewege verbindlich festgelegt?
- ☑ Können Teams die für Erstmeldung, Zwischenbericht und Abschlussbericht nötigen Informationen zeitnah zusammentragen?
- ☑ Werden Ursachen, Auswirkungen, getroffene Maßnahmen und Lessons Learned nachvollziehbar dokumentiert?
- ☑ Werden Meldepflichten regelmäßig geübt, damit sie auch unter Zeitdruck funktionieren?

NACHWEISE

- Incident-Response-Prozess und Eskalationsmatrix
- Klassifizierungskriterien für Vorfälle
- Meldeformulare, Vorlagen und Kontaktlisten
- Vorfallsdokumentationen und Nachbesprechungen

4 Tests der digitalen operationalen Resilienz

DORA verlangt regelmäßige Tests von IKT-Werkzeugen, Systemen und Prozessen. Ziel ist nicht nur ein Testnachweis, sondern der Beleg, dass Kontrollen, Reaktionswege und Wiederanlauf im Ernstfall tragen.

CHECKPUNKTE

- [ ] Gibt es ein dokumentiertes Testprogramm mit Umfang, Frequenz und Verantwortlichkeiten?
- [ ] Werden technische Kontrollen, Wiederherstellungsverfahren und Notfallprozesse regelmäßig getestet?
- [ ] Sind kritische Systeme und Prozesse im Testumfang enthalten?
- [ ] Werden Ergebnisse, Abweichungen und Maßnahmen systematisch dokumentiert?
- [ ] Gibt es klare Fristen für die Behebung festgestellter Schwächen?
- [ ] Werden Testergebnisse in Risikoanalysen und Verbesserungsmaßnahmen zurückgeführt?
- [ ] Ist geprüft, ob für Ihr Institut zusätzliche fortgeschrittene Testanforderungen relevant sind?

NACHWEISE

- Testpläne und Testkalender
- Ergebnisse aus Notfalltests, Wiederanlauftests oder technischen Prüfungen
- Maßnahmenlisten mit Status
- Management-Berichte zu Testbefunden

5 IKT-Drittdienstleister und Informationsregister

DORA verlangt ein belastbares Management von IKT-Drittdienstleister-Risiken. Dazu gehört auch ein umfassendes Register zu vertraglichen Vereinbarungen mit IKT-Drittdienstleistern, das für Aufsicht und Steuerung nutzbar ist.

CHECKPUNKTE

- ☑ Ist vollständig erfasst, welche IKT-Drittdienstleister für welche Leistungen eingesetzt werden?
- ☑ Sind kritische oder wichtige Funktionen eindeutig gekennzeichnet?
- ☑ Sind Abhängigkeiten, Unterauftragnehmer und Konzentrationsrisiken sichtbar?
- ☑ Liegen aktuelle Verträge mit den nötigen Regelungen zu Sicherheit, Zugriff, Audit, Unterstützung und Exit vor?
- ☑ Gibt es einen klaren Prozess für Auswahl, Bewertung, Freigabe und laufende Überwachung von Anbietern?
- ☑ Wird das Informationsregister regelmäßig aktualisiert und qualitätsgesichert?
- ☑ Sind Exit-Strategien für kritische Leistungen dokumentiert und realistisch umsetzbar?

NACHWEISE

- Register der Informations- und Vertragsbeziehungen
- Anbieterbewertungen und Risikoeinstufungen
- Vertragsunterlagen und Kontrollnachweise
- Exit-Pläne und Übersichten zu Subdienstleistern

6 Human Risk Management und Security Awareness

DORA adressiert zwar vor allem Governance, Risiken, Vorfälle, Tests und Drittparteien. In der Praxis scheitern Kontrollen jedoch oft an menschlichen Fehlern, unklaren Zuständigkeiten oder unsicheren Entscheidungen. Für Head of IT ist dieser Bereich deshalb operativ relevant, auch wenn er in DORA nicht als eigenes Hauptkapitel geführt wird.

CHECKPUNKTE

- ☑ Wissen Mitarbeitende, wie sie Phishing, Social Engineering und verdächtige Anfragen erkennen?
- ☑ Kennen sie den richtigen Meldeweg für Sicherheitsvorfälle und Auffälligkeiten?
- ☑ Sind Awareness-Maßnahmen auf Zielgruppen, Risiken und Rollen zugeschnitten?
- ☑ Werden besonders exponierte Gruppen gezielt geschult, etwa Helpdesk, Finance oder Admin-Teams?
- ☑ Werden Trainings, Phishing-Simulationen oder Kommunikationsmaßnahmen ausgewertet?
- ☑ Fließen typische Fehlermuster in technische und organisatorische Schutzmaßnahmen zurück?
- ☑ Ist klar geregelt, wie Security Awareness mit Incident Response und Risikomanagement zusammenwirkt?

NACHWEISE

- Schulungskonzepte und Teilnahmequoten
- Ergebnisse aus Simulationen oder Lernformaten
- Kommunikationspläne und Meldehinweise
- Maßnahmen aus Lessons Learned

7 Dokumentation und Nachweisfähigkeit

DORA-Compliance scheitert in der Praxis oft nicht nur an fehlenden Maßnahmen, sondern an fehlender Nachweisfähigkeit. Für Prüfungen zählt, ob Anforderungen nachvollziehbar dokumentiert, aktuell gepflegt und bei Bedarf schnell verfügbar sind.

CHECKPUNKTE

- [x] Sind zentrale Richtlinien, Prozesse und Nachweise vollständig und aktuell?
- [x] Gibt es klare Eigentümer für Dokumente und Register?
- [x] Werden Versionen, Freigaben und Änderungen nachvollziehbar gepflegt?
- [x] Können Nachweise innerhalb kurzer Zeit bereitgestellt werden?
- [x] Ist dokumentiert, wie Maßnahmen, Ausnahmen und Restrisiken entschieden wurden?
- [x] Sind Überschneidungen zwischen IT, Security, Risk und Compliance sauber abgestimmt?

NACHWEISE

- Dokumentenlenkung und Freigabelisten
- Prozessdokumentationen und Verfahrensanweisungen
- Prüfpfade, Review-Historien und Maßnahmenprotokolle

Priorisierung für die erste Lückenanalyse

Nicht jede Lücke hat das gleiche Gewicht. Für eine erste Einordnung helfen drei Prioritätsfragen:

- ☑ Betrifft die Lücke einen kritischen Prozess oder eine wichtige Funktion?
- ☑ Erhöht die Lücke das Risiko eines schweren IKT-Vorfalls oder einer verspäteten Meldung?
- ☑ Fehlt ein Nachweis, der in einer Prüfung unmittelbar relevant wäre?

Wenn Sie eine dieser Fragen mit Ja beantworten, sollte der Punkt kurzfristig priorisiert werden.

Arbeitsvorlage für die interne Bewertung

Prüffeld	Status	Risiko bei Lücke	Nächste Maßnahme	Verantwortlich	Zieltermin
Governance					
IKT-Risikomanagement					
Vorfallmanagement					
Resilienztests					
IKT-Drittdienstleister					
Human Risk Management					
Dokumentation					

Für die Praxis

Die Checkliste ist besonders nützlich, wenn sie nicht isoliert von einem Team ausgefüllt wird. Gute Ergebnisse entstehen dort, wo IT, Informationssicherheit, Risikomanagement, Compliance und relevante Fachbereiche gemeinsam auf denselben Umsetzungsstand blicken. So werden Lücken früher sichtbar und Maßnahmen schneller belastbar.