

DORA-Nachweis-Checkliste für IT-Service-Management

Welche Belege in Prüfungen tatsächlich verlangt werden

Diese Liste ist eine fachliche Arbeitshilfe für IT-Service-Management-Verantwortliche. Sie ist weder Rechtsberatung noch eine vollständige Darstellung der Verordnung; maßgeblich sind die Verordnung selbst und die Vorgaben Ihrer Aufsicht. Erfahrungsgemäß wird in Prüfungen weniger die Existenz eines Prozesses geprüft als dessen Nachweisbarkeit am Einzelfall.

1 Kritische Funktionen und Assets

- ☐ Kritische und wichtige Funktionen sind fachlich hergeleitet und dokumentiert.
- ☐ Die Herleitung ist nachvollziehbar und mit den Fachbereichen abgestimmt.
- ☐ IKT-Assets sind diesen Funktionen zugeordnet.
- ☐ Die Zuordnung wird gepflegt und ihre Qualität wird geprüft.
- ☐ Änderungen an kritischen Funktionen folgen einem definierten Verfahren.

2 Störungsbearbeitung und Meldung

- ☐ Klassifizierungskriterien für Vorfälle sind dokumentiert und werden angewandt.
- ☐ Ein Prozess für schwerwiegende Vorfälle ist beschrieben und geübt.
- ☐ Die Kriterien für die Einstufung als meldepflichtig sind hinterlegt.
- ☐ Vorlagen für Erst-, Zwischen- und Abschlussmeldung liegen vor.
- ☐ Zuständigkeiten und Fristen für Meldungen sind benannt.
- ☐ Übungen und reale Fälle sind protokolliert.

3 Änderungen

- ☐ Changes sind risikobasiert klassifiziert.
- ☐ Freigaben sind dokumentiert und nachvollziehbar.
- ☐ Die Prüfung der Auswirkung auf kritische Funktionen ist fester Prozessschritt.
- ☐ Notfalländerungen folgen einem Verfahren mit verbindlicher Nachdokumentation.
- ☐ Eine Stichprobe lässt sich lückenlos von Antrag bis Umsetzung verfolgen.

4 IKT-Drittdienstleister

- ☐ Das Informationsregister ist vollständig, einschließlich Unterauftragsverhältnissen.
- ☐ Kritische Dienstleister sind eingestuft, die Kriterien sind dokumentiert.
- ☐ Verträge enthalten die geforderten Regelungen zu Prüfung, Zugang und Beendigung.
- ☐ Ausstiegsstrategien liegen vor, mit Szenario, Zeitbedarf und Zielbild.
- ☐ Die Leistung wird laufend überwacht und berichtet.
- ☐ Konzentrationsrisiken sind bewertet.

5 Fortführung und Tests

- ☐ Wiederanlaufpläne bestehen je kritischer Funktion.
- ☐ Wiederanlaufziele sind festgelegt und mit dem Fachbereich abgestimmt.
- ☐ Tests finden in festem Turnus statt und sind protokolliert.
- ☐ Feststellungen aus Tests werden nachverfolgt bis zur Erledigung.
- ☐ Szenarien umfassen auch den Ausfall eines kritischen Dienstleisters.

6 Steuerung und Berichtswesen

- ☐ Der IKT-Risikorahmen ist verabschiedet und die Verantwortung ist zugeordnet.
- ☐ Das Leitungsorgan erhält regelmäßig ein Risikoberichtswesen.
- ☐ Schwachstellen werden erfasst, bewertet und fristgebunden behandelt.
- ☐ Entscheidungen und Abweichungen sind prüfbar dokumentiert.
- ☐ Die Wirksamkeit der Prozesse wird regelmäßig überprüft.

FRAGEN ZU DIESER CHECKLISTE?

Christian Heitzer

Interim IT-Projektleitung, Transition und ITSM in regulierten Umgebungen
heitzer.info · +49 6142 4769-324

Diese Checkliste ist eine fachliche Arbeitshilfe und ersetzt keine Rechts-, Steuer- oder aufsichtsrechtliche Beratung. Die Anwendbarkeit einzelner Punkte hängt vom konkreten Vorhaben ab.

