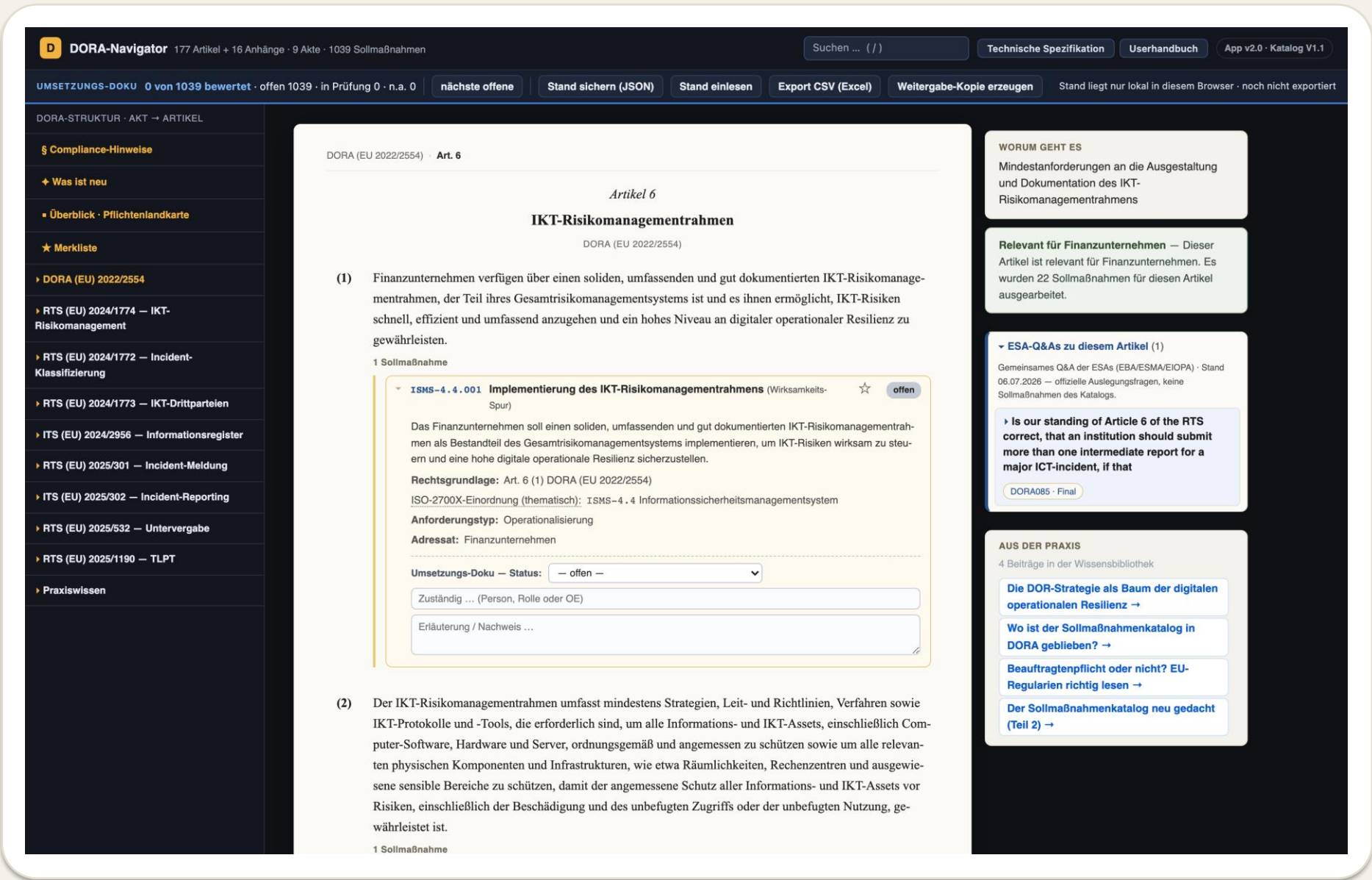


Erste Einblicke

Der DORA-Navigator

Ein interaktives DORA-Handbuch: Rechtstexte, Sollmaßnahmen, die FAQs der ESAs und zwei Jahre Praxiswissen — in einer einzigen HTML-Datei.

Drei Spalten, ein Zusammenhang.



Links die Struktur der Rechtsakte, in der Mitte Rechtstext und abgeleitete Sollmaßnahme, rechts der Kontext — Auslegung, ESA-FAQ, Praxiswissen. Alles in einer HTML-Datei.

1.039 Sollmaßnahmen. Eine Struktur.

Sollmaßnahmen-Statistik



Anforderungstyp	Sollmaßnahmen
Operationalisierung	440
Richtlinie	263
Verfahren	213
Vertrag	36
Technisches Konzept	30
Plan	24
Bericht	21
Strategie	12

Alle DORA-Anforderungen als atomare Arbeitseinheiten — geordnet in der ISO 27001-Struktur.

Vom Rechtstext zur Sollmaßnahme.

DORA (EU 2022/2554) › Art. 6

Artikel 6

IKT-Risikomanagementrahmen

DORA (EU 2022/2554)

- (1) Finanzunternehmen verfügen über einen soliden, umfassenden und gut dokumentierten IKT-Risikomanagementrahmen, der Teil ihres Gesamtrisikomanagementsystems ist und es ihnen ermöglicht, IKT-Risiken schnell, effizient und umfassend anzugehen und ein hohes Niveau an digitaler operativer Resilienz zu gewährleisten.

1 Sollmaßnahme

- ▼ **ISMS-4.4.001 Implementierung des IKT-Risikomanagementrahmens** (Wirksamkeits-Spur) ☆ **offen**

Das Finanzunternehmen soll einen soliden, umfassenden und gut dokumentierten IKT-Risikomanagementrahmen als Bestandteil des Gesamtrisikomanagementsystems implementieren, um IKT-Risiken wirksam zu steuern und eine hohe digitale operationale Resilienz sicherzustellen.

Rechtsgrundlage: Art. 6 (1) DORA (EU 2022/2554)

ISO-2700X-Einordnung (thematisch): ISMS-4.4 Informationssicherheitsmanagementsystem

Anforderungstyp: Operationalisierung

Adressat: Finanzunternehmen

Der amtliche Wortlaut und die daraus abgeleitete Sollmaßnahme — direkt untereinander, Absatz für Absatz.

Status. Verantwortlicher. Nachweis.

▼ ISMS-4.4.001 Implementierung des IKT-Risikomanagementrahmens



Vollständig (4)

(Wirksamkeits-Spur)

Das Finanzunternehmen soll einen soliden, umfassenden und gut dokumentierten IKT-Risikomanagementrahmen als Bestandteil des Gesamtrisikomanagementsystems implementieren, um IKT-Risiken wirksam zu steuern und eine hohe digitale operationale Resilienz sicherzustellen.

Rechtsgrundlage: Art. 6 (1) DORA (EU 2022/2554)

ISO-2700X-Einordnung (thematisch): ISMS-4.4 Informationssicherheitsmanagementsystem

Anforderungstyp: Operationalisierung

Adressat: Finanzunternehmen

Umsetzungs-Doku — Status:

Vollständig vorhanden/compliant (4 Pkt)



ISB · Team IKT-Governance

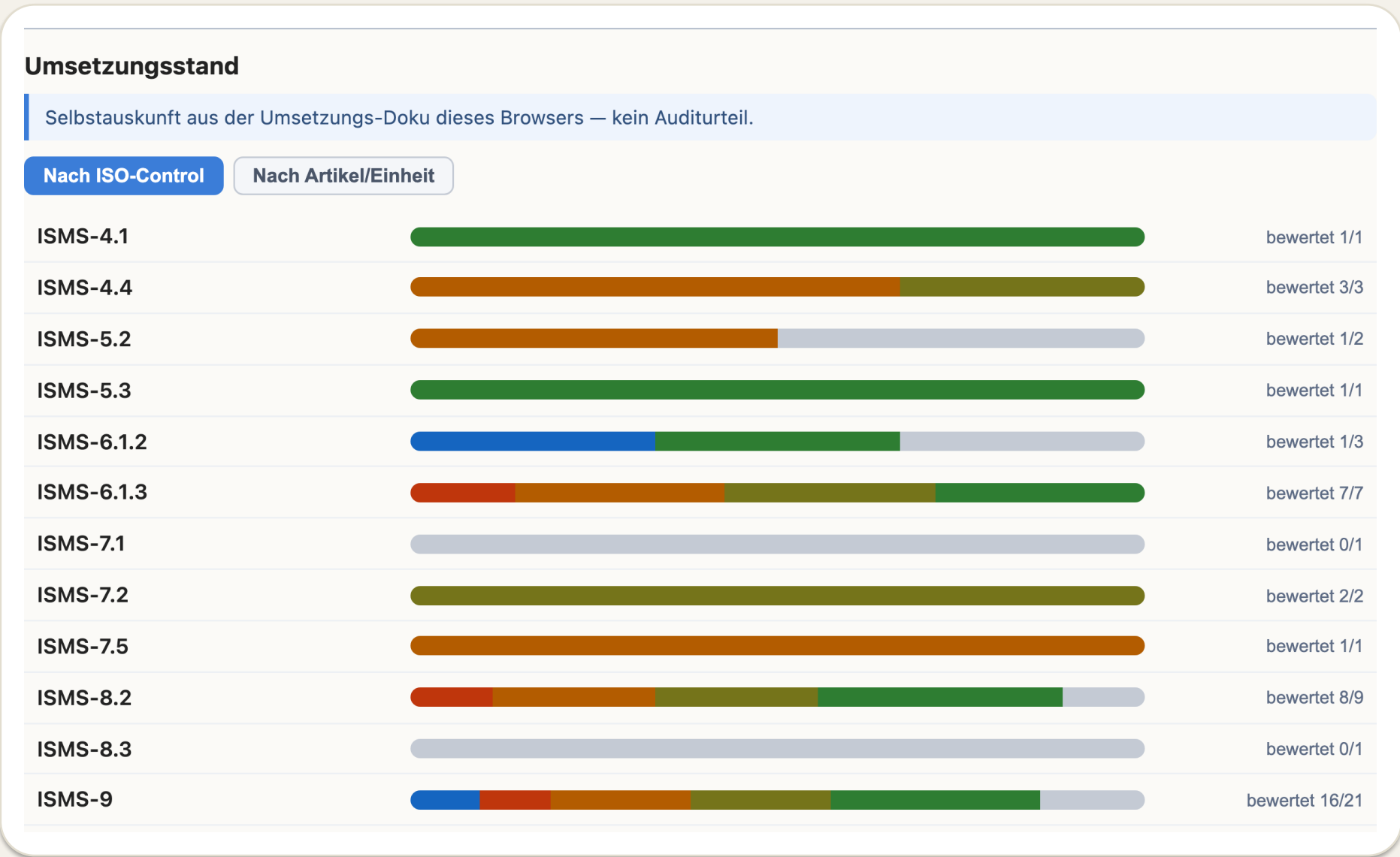
Umgesetzt über die IKT-Risikomanagement-Richtlinie v3.2 (Kap. 4). Nachweis: Freigabe Leitungsorgan 03/2026, Revisionsbericht IR-2026-014.



Stand der Einstufung: 2026-07-17

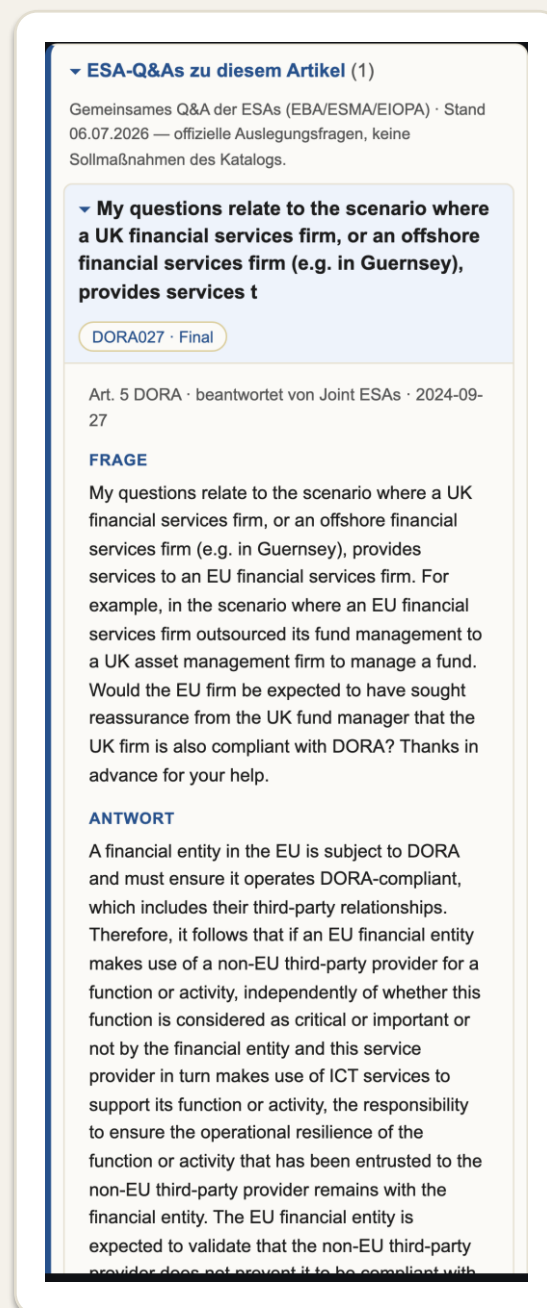
Zu jeder Sollmaßnahme: Umsetzungsstand, wer zuständig ist und womit es belegt wird — genau die Fragen einer Prüfung.

Wo steht das Unternehmen?



Der Umsetzungsstand, verdichtet in ISO 27001-Struktur — Non-Compliance-Risiken werden auf einen Blick sichtbar.

Die FAQs der ESAs — am Artikel.



Die offiziellen Auslegungsfragen von EBA, ESMA und EIOPA, dort verortet, wo sie gebraucht werden.

Praxiswissen, eingebaut.

Praxiswissen › Wer erstellt und aktualisiert die 17 IKT-Sicherheitsrichtli...

Praxiswissen

Wer erstellt und aktualisiert die 17 IKT-Sicherheitsrichtlinien?

WISSENSBIBLIOTHEK — DORA-NAVIGATOR

BEITRAG

Wer erstellt und aktualisiert die 17 IKT-Sicherheitsrichtlinien?

Quelle: [LinkedIn](#) · 2024-12-05

In einem früheren Artikel habe ich den DORA-Tempel vorgestellt, der 17 themenspezifische IKT-Sicherheitsrichtlinien umfasst. Diese decken eine breite Palette von Fachthemen ab – von IT-Betriebssicherheit über Projektmanagement bis hin zur Personalsicherheit. Doch eine zentrale Frage bleibt: Wer ist eigentlich verantwortlich für das Erstellen und Aktualisieren dieser Richtlinien?

Die Diskussionen, sowohl hier im Netzwerk als auch in den Unternehmen, zeigen, dass diese Frage alles andere als einfach ist. Es geht um verfügbare Kapazitäten, fachliche Expertise und nicht zuletzt um die Frage, wer im Unternehmen die Befugnis hat, solche Vorgaben zu erstellen. Die Verantwortung dafür liegt letztlich beim Leitungsorgan, das sicherstellen muss, dass die erforderlichen IKT-Sicherheitsrichtlinien vorhanden sind. Aber wie wird diese Aufgabe intern verteilt?

Das BSI weist unter anderem darauf hin, dass der Informationssicherheitsbeauftragte (ISB) für die Erstellung der Informationssicherheitsleitlinie verantwortlich ist. Darüber hinaus zählt zu seinen Aufgaben, „die Erstellung des Sicherheitskonzepts und zugehöriger Teilkonzepte und Richtlinien zu koordinieren.“ Diese

Meine Fachbeiträge zu den Artikeln, mit denen sie zusammenhängen — nicht in irgendeinem Ordner, nicht auf LinkedIn, sondern am Text.

Aus dem Katalog wird ein Arbeitsinstrument.

Der DORA-Navigator wird das nächste Produkt aus meiner DORA-Werkstatt.

**Schreibt mir hier auf LinkedIn
oder über meine Website, wenn ihr mehr sehen möchtet.**