Überblick aktueller gesetzlicher Vorgaben aus dem Blickwinkel Finanzdienstleister, Banken & Versicherungen

BIESER

	Stabilität & Resilienz		Cybersicherheit	
Kriterium	***EU DORA (Jan 23) DE FinmaDiG (Okt 24)***	***EU CER (Dez 22) DE KRITIS Dachgesetz (Okt 24)***	***EU NIS-2 (Jan 23) DE NIS2UmsuCG (Okt 24)***	***IT-Sicherheitsgesetz 2.0 (Mai 2021)***
Art & Herausgeber	Verordnung der Europäischen Union (ohne nationale Gesetzgebung gültig) in Deutschland trotzdem konkretisiert durch: Finanzmarktdigitalisierungsgesetz	Richtlinie der Europäischen Union mit Bedarf nach nationaler Umsetzung. Deutsches Gesetz: KRITIS Dachgesetz	Richtlinie der Europäischen Union mit Bedarf nach nationaler Umsetzung. Deutsches Gesetz: NIS2-Umsetzungs und Cybersicherheits-Gesetz	Bundesministerium des Innern, für Bau und Heimat (BMI), Deutschland
Geltungsbereich Finanzwesen	Finanzsektor, einschließlich Banken, Versicherungen, Investmentfirmen und Krypto-Dienstleister, Börsen, FDL, etc.	KRITIS Betreiber	KRITIS + 18 Sektoren & Unternehmensgröße Die von DORA regulierten Finanzunternehmen sind von fast allen NIS2-Pflichten (bis auf Registrierung beim BSI) ausgenommen, wenn sie in DORA reguliert sind (lex specialis)	KRITIS-Betreiber
Ziel	**Verbesserung der digitalen operativen Resilienz und Sicherstellung der Stabilität des Finanzsystems in der EU**	**Schutz kritischer Einrichtungen, Ausfallsicherheit. Resilienzpläne im Rahmen der betrieblichen Gesamtresilienzstrategie**	**Stärkung der Cybersicherheit, Verbesserung der Widerstandsfähigkeit und des Umgangs mit Cybervorfällen**	**Verbesserung der Cybersicherheit und Schutz kritischer Infrastrukturen in Deutschland**
Zusammenhang	Ergänzt andere EU-Verordnungen im Finanzsektor wie MiFID II und PSD2, BAIT soll ggfs. in DORA aufgehen, DORA wird über FinmaDiG in Deutschland konkretisiert.	BSI Gesetz (2015) KRITIS Verordnung IT-Sicherheitgesetz 2.0 (2021)	Ergänzt und erweitert die ursprüngliche NIS-Richtlinie. NIS-1 (Vorgänger). Wird in Deutschland umgesetzt im NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)	Baut auf BSI-Gesetz auf und KRITIS-Verordnung Grundlage für andere spezifische Regelwerke wie KRITIS und BAIT Nimmt zum Teil NIS-2 vorweg
Zeitliche Perspektive	Vorgaben müssen von Betroffenen bis 17. Januar 2025 umgesetzt sein	Spätestens bis 17.07.2026	2016 (NIS), Überarbeitung als NIS-2 in 2022. Gesetz tritt voraussichtlich im Oktober 2024 in Kraft.	2009, überarbeitet 2015 (IT-Sicherheitsgesetz 2.0 in 2021)
Inhalt	Risikomanagementsystem wird Pflicht für IKT, Strenge Meldepflichten für IKT-bezogene Vorfälle, Regelmäßige Tests der digitalen Resilienz, Management der IKT-Drittanbieter-Risiken. Managementverantwortung für IKT-Risiken.	Erstmals Regelung zum physischen Schutz, betr. Resilienzmanagement, insb. Einrichtung eines betrieblichen Risiko- und Krisenmanagements; Erstellung von Resilienzplänen. Erweiterte Meldepflichten und Befugnisse des BBK zu Audits.	Maßnahmen zur Risikomanagement, ISMS, Meldepflichten für Vorfälle, nationale Aufsichtsbehörden, EU-weite Zusammenarbeit Erweiterte Befugnisse des BSI (z.B. vor Ort Kontrollen)	Maßnahmen zur Verbesserung der IT-Sicherheit, Schutz kritischer Infrastrukturen, Meldepflichten für Sicherheitsvorfälle Erweiterte Befugnisse des BSI (Anordnung zur Behebung von Sicherheitslücken) Einführung IT-Sicherheitskennzeichen
Sanktionen	10 Mio EUR / 5% Vorjahresumsatz IKT-Drittdienstleister: 1% des durchschnittlichen weltweiten Tagesumsatz/Tag	Hängt von kommender Gesetzgebung ab	0,1 – 10 Mio. EUR oder globalem Umsatz, je nach Sektor	0,1 – 20 Mio. EUR

© 2024 Christian Bieser | Bieser IT Consulting