Norm / Standard	Rechtsnatur	Status	Relevante Passage	Was tatsächlich gefordert wird
NIS-2	EU-Richtlinie 2022/2555	In nationales Recht umzusetzen; in Deutschland durch BSIG konkretisiert	Art. 21 Abs. 2 lit. b, f	Bewältigung von Sicherheitsvorfällen; Verfahren zur Bewertung der Wirksamkeit von Sicherheitsmaßnahmen; geeignete technische und organisatorische Maßnahmen erforderlich; keine SOC-Vorgabe
NIS-2-Durchführungsrechtsakt	EU-Verordnung 2024/2690	Anwendbar seit 17.10.2024	Anhang: technische und methodische Anforderungen	Konkretisierung technischer Maßnahmen für DNS, Cloud, Rechenzentren et cetera; Fähigkeiten und Prozesse gefordert; keine SOC-Vorgabe
BSIG (neue Fassung)	Deutsches Gesetz	Seit 06.12.2025 in Kraft	§§ 30, 32, 38	Risikomanagement in zehn Bereichen (§ 30); Meldefristen 24h/72h/1 Monat (§ 32); Governance und persönliche Haftung der Geschäftsleitung (§ 38); keine SOC-Vorgabe
DORA	EU-Verordnung 2022/2554	Anwendbar seit 17.01.2025	Art. 10	Mechanismen zur zeitnahen Erkennung anomaler Aktivitäten; mehrere Kontrollebenen; automatische Warnungen; Funktionalität gefordert, keine SOC-Vorgabe
DORA	EU-Verordnung 2022/2554	Anwendbar seit 17.01.2025	Art. 17–19 i. V. m. RTS 2024/1772	IKT-Vorfallmanagement, Klassifizierung, Meldung mit Fristen; Prozesse erforderlich; Umsetzung intern/extern/hybrid möglich
CRA	EU-Verordnung 2024/2847	Meldepflicht ab 11.09.2026	Art. 14	Meldung aktiv ausgenutzter Schwachstellen und schwerer Vorfälle: 24 h, 72 h, 14 Tage. Funktions- und Meldepflichten; keine SOC-Vorgabe
CRA	EU-Verordnung 2024/2847	Vollanwendung ab 11.12.2027	Art. 13, Anhang I	Security-by-Design, Vulnerability Handling über Produktlebenszyklus, CE-Konformität; Produktsicherheit gefordert, keine SOC-Vorgabe
KRITIS-Dachgesetz	Deutsches Gesetz	Beschlossen 29.01.2026, in Kraft seit 16.03.2026	Umsetzung RL EU 2022/2557	physische und organisatorische Resilienz kritischer Anlage. Resilienzfähigkeit gefordert; keine SOC-Vorgabe
ISO/IEC 27001:2022	Internationale Norm	Zertifizierbar	Annex A 8.16	Monitoring-Aktivitäten in Netzen, Systemen, Anwendungen; Kontrollen erforderlich; keine SOC-Vorgabe
ISO/IEC 27001:2022	Internationale Norm	Zertifizierbar	Annex A 5.24–5.28	Incident-Management-Lifecycle: Planung, Bewertung, Reaktion, Lessons Learned, Beweissicherung; Prozesse gefordert; keine SOC-Vorgabe
NIST CSF 2.0	Internationales Framework	Freiwilliger Referenzrahmen	Functions DE, RS	Detect, Respond als Funktionen; Fähigkeiten beschrieben; keine SOC-Vorgabe