Fristen-Kalender

Der folgende Kalender stellt die wesentlichen regulatorischen Fristen und Umsetzungsmeilensteine strukturiert dar. Er dient als operative Grundlage für Planung, Priorisierung und Steuerung.

2024 (bereits laufend)

- Inkrafttreten der NIS-2-Richtlinie auf EU-Ebene
- Inkrafttreten DORA (EU-Verordnung)
- Beginn Übergangsphase für nationale Umsetzung (NIS-2)
- Start erster Betroffenheitsanalysen und Gap-Analysen
- Aufbau initialer Governance- und Risikostrukturen

2025 (Umsetzungsstart / Strukturaufbau)

Q1–Q2 2025

- Abschluss Betroffenheitsanalyse (NIS-2, DORA, CRA, EU AI Act)
- Definition Governance-Struktur und Rollenmodell
- Aufbau Risikomanagement-Framework
- Start KI-Inventur

Q3–Q4 2025

- Einführung Incident-Response-Prozesse
- Aufbau Meldeprozesse (inkl. Fristenlogik)
- Start Tool-Auswahl (GRC, Security, TPRM, AI Governance)
- Beginn Lieferkettenbewertungen (Vendor Risk Management)

2026 (Kritisches Umsetzungsjahr / regulatorischer Druck steigt)

Q1 2026

- Finalisierung NIS-2-Umsetzung auf nationaler Ebene
- Etablierung Meldeketten und Reporting-Strukturen
- Erste interne Audits / Readiness Checks

Q2 2026

- Vollständige Implementierung Incident Response
- Integration Security Operations (SIEM / SOAR / EDR)
- Aufbau Evidence Management

Q3 2026

- Erste verpflichtende Anforderungen aus dem EU AI Act
- Einführung KI-Governance-Strukturen
- Start KI-Risikoklassifizierung

Q4 2026

- Erwartete erste regulatorische Prüfungen
- Hoher Bedarf an Audit-Nachweisen
- Auditoren-Engpass möglich
- Abschluss initialer Implementierungsphase

2027 (Erweiterung / Prüfungsphase)

Q1–Q2 2027

- Erweiterte Anforderungen EU AI Act (insbesondere Hochrisiko-KI)
- Ausbau Dokumentation und Konformitätsbewertungen
- Integration SBOM und CRA-Anforderungen

Q3–Q4 2027

- Verstärkte Audits durch Aufsichtsbehörden
- Optimierung von Prozessen und Kontrollen
- Erweiterung Automatisierung und Integration

2028 (Stabilisierungs- und Optimierungsphase)

- Vollständige operative Wirksamkeit aller Regulierungen
- Etablierung von Continuous Compliance
- KPI-basierte Steuerung und Monitoring
- Integration neuer regulatorischer Anforderungen
- Fokus auf Effizienz, Skalierung und Resilienz

Dauerhafte Fristen (laufend relevant)

- Incident-Meldungen innerhalb regulatorischer Zeitfenster
- Regelmäßige Risikobewertungen
- Kontinuierliche Schulungen und Awareness
- Wiederkehrende Audits und Nachweisführung

}

Mehr zum Thema Automated Compliance Monitoring

Der vollständige Leitfaden „Automated Compliance Monitoring – Kontinuierliche Auditfähigkeit für NIS2, DORA, CRA und EU AI Act“