DAVID ZION · vCISO UND STRATEGISCHE BERATUNG

Gap-Analyse ISO 27001 / NIS2

Standortbestimmung · zehn Themenfelder · Reifegrad 0 bis 5 · priorisierte Roadmap

davidzion.de · kontakt@davidzion.de · Hamburg (+100 km) und remote

Wo stehen Sie, was fehlt und was ist zuerst zu tun. Ich bewerte Ihr Unternehmen entlang von zehn Themenfeldern, bei NIS2 den Maßnahmenbereichen nach § 30 BSIG, bei ISO 27001 im Abgleich mit Annex A. Grundlage sind Ihre Unterlagen und Interviews mit den Verantwortlichen. Zielniveau ist Reifegrad 3, also definiert und gelebt.

ERGEBNIS

- **Management-Summary** auf zwei Seiten für Geschäftsleitung und Gesellschafter
- **Reifegrad-Radar** mit Scores zu allen Themenfeldern
- **Gap-Liste** je Themenfeld, konkret und belegt
- **Priorisierte Roadmap:** Sofortmaßnahmen, 90-Tage-Plan und 12-Monats-Horizont
- **Beschlussvorlage** für die Leitung, bei NIS2 zur Dokumentation der Umsetzungs- und Überwachungsentscheidung nach § 38 BSIG

ABLAUF IN DREI WOCHEN

- **Tag 1 bis 3:** Kickoff, Scoping, Sichtung der Unterlagen
- **Woche 1 bis 2:** Interviews zu je 60 Minuten
- **Woche 2:** Bewertung und Reifegradermittlung
- **Woche 3:** Ergebnispräsentation vor der Geschäftsleitung

NICHT ENTHALTEN

- technische Prüfungen wie Penetrationstest oder Schwachstellenscan, die Umsetzung der Maßnahmen und das Zertifizierungsaudit. Diese folgen als eigener Schritt oder im vCISO-Retainer.

PAKETE ZUM FESTPREIS, JE REGELWERK

- **Paket S:** 1 Standort, 9.500 €
- **Paket M:** bis 2 Standorte, 12.500 €
- **Paket L:** bis 3 Standorte, 16.500 €
- **ISO 27001 und NIS2 zusammen:** + 3.500 € auf den Paketpreis

Beispiel Paket S für beide Regelwerke: 9.500 € + 3.500 € = 13.000 €. Welches Paket passt, klären wir im Erstgespräch.

IHR AUFWAND UND DIE NÄCHSTEN SCHRITTE

- **Ihr Aufwand:** ein Ansprechpartner, Zugang zu den Unterlagen, Interviewtermine
- **KI-Governance-Check dazu:** + 4.500 € statt 6.500 €, weil Interviews und Sichtung nur einmal anfallen
- **Umsetzung der Roadmap** im vCISO-Retainer, Security-Beirat ab 2.500 € im Monat

Über 40 Jahre in der IT, davon mehr als 30 in Führungsverantwortung
CISM · ISO/IEC 27001 Lead Implementer · ISO/IEC 42001 KI-Manager · AI Compliance nach EU AI Act

Erstgespräch: 30 Minuten, kostenfrei · Angebot binnen 48 Stunden · davidzion.de

Stand 19. November 2026. Alle Preise netto zzgl. MwSt. Die Angaben zur Rechtslage ersetzen keine Rechtsberatung.