



CISO AS A SERVICE.

Managed Service • Dauermandat **info@doitag.de**

Sie brauchen die Sicherheitsfunktion besetzt, nicht eine weitere Stelle ausgeschrieben. Wir stellen den Informationssicherheitsbeauftragten, liefern die Führungsinstrumente und führen den Nachweis – dauerhaft, zum festen Monatspreis.

01. Besetzte Rolle statt offener Stelle

im Dauermandat

Benannter Informationssicherheitsbeauftragter mit vereinbarter Verfügbarkeit, festem Ansprechpartner und Vertretungsregelung. Nach außen eine Person, nach innen ein Team mit Architektur-, Betriebs- und Regulatorikkompetenz.

Ergebnis: dauerhaft besetzte Funktion, dokumentierte Bestellung und Erreichbarkeit

02. Führungsinstrumente und Schulung der Leitung

im Dauermandat

Risikoregister, priorisierter Maßnahmenplan und Quartalsbericht, aufbereitet als Beschlussvorlage. Dazu die regelmäßige Schulung der Geschäftsleitung mit Teilnahmenachweis, zugeschnitten auf Ihre Systeme statt auf allgemeine Folien.

Ergebnis: dokumentierte Billigung, laufende Überwachung und Schulungsnachweis nach § 38 BSIG

03. Audit-Defence: Nachweisbestand und Begleitung

Bereitschaft inklusive

Wir halten die Evidenzmappe aktuell, prüfen im Probeaudit mit den Augen des Prüfers und begleiten Zertifizierungs-, Nachweis- und Kundenaudits bis zum Abschluss des Feststellungsmanagements. Wer erst bei der Ankündigung sucht, hat schon verloren.

Ergebnis: jederzeit vorzeigbarer Nachweisbestand, abgearbeitete Feststellungen

04. Lieferanten, Dritte und laufende Steuerung

im Dauermandat

Bewertung Ihrer Dienstleister, Bearbeitung eingehender Sicherheitsfragebögen, Sicherheitsanforderungen in Verträgen sowie die Steuerung der laufenden Maßnahmen zwischen den Berichtsterminen. Für Finanzunternehmen führen wir zusätzlich das Informationsregister und das Management der IKT-Drittparteienrisiken nach DORA.

Ergebnis: bewertetes Lieferantenportfolio und nachverfolgte Maßnahmenumsetzung

05. KI-Governance im laufenden Betrieb

KI & Automatisierung

Nutzungsregeln für KI-Dienste, ein Freigabeverfahren für neue Werkzeuge und ein fortgeschriebenes Register der Handlungsträger. Einmal jährlich prüfen wir die Delegationsketten gegen den dokumentierten Stand und berichten der Geschäftsleitung, was sich verändert hat.

Ergebnis: KI-Richtlinie, Freigabeverfahren und jährlich geprüfetes Register der automatisierten Handlungsträger

Drei Servicestufen – Kompakt, Standard und Intensiv. Den Umfang legen wir nach der Bestandsaufnahme fest.

Dauermandat

So läuft es ab

1. Bestandsaufnahme, Festlegung der Servicestufe und Bestellung des Beauftragten.
2. Fester Turnus aus Jour fixe, Quartalsbericht und jährlicher Schulung der Leitung.
3. Bei Prüfungen Wechsel in den Audit-Defence-Modus, im Vorfall Übergabe an Angebot 04.

Was wir von Ihnen brauchen

- Mandat und Zugang zur Geschäftsleitung, nicht nur zur IT.
- Eine interne Person, die operative Umsetzungen anstoßen kann.
- Mindestlaufzeit zwölf Monate, danach quartalsweise kündbar.

Was wir ausdrücklich nicht übernehmen

Die Billigung der Maßnahmen, die Überwachungspflicht und die persönliche Haftung der Geschäftsleitung bleiben bei Ihnen – daran kann kein Dienstleistungsvertrag etwas ändern. **Wer Ihnen das Gegenteil verspricht, verkauft Ihnen ein Risiko.**

Wir liefern die Entscheidungsgrundlage, die Dokumentation und den Nachweis, dass Sie entschieden haben. Genau das ist es, was im Prüfungs- und im Haftungsfall zählt.