

Thorsten Franz

COMPLIANCE & AUDIT

Ausgeschrieben als: Compliance Manager IT · Projektleiter ISO 27001 / BSI C5 · IT-Compliance Consultant

info@franz.com.de · franz.com.de
+357 96017744 · +49 1590 6826228



• VERFÜGBAR — DACH, CY, REMOTE & VOR ORT — DIREKTVERTRAG

Ein Testat entsteht nicht aus Dokumenten, sondern aus Entscheidungen

Auf der Cloud-Plattform eines internationalen Handelskonzerns habe ich das BSI-C5-Programm der Organisation bis zur Prüfungsreife geführt, mit einer Big-Four-Wirtschaftsprüfungsgesellschaft als externem Prüfer – den vollständigen Kriterienkatalog Kriterium für Kriterium mit dem Prüfer durchgegangen, Auslegung geklärt, Prüfbedingungen und Nachweiserwartung je Control vereinbart. Das Testat wurde erreicht, nach meiner Übergabe in der letzten Phase.

1.

BSI-C5-TESTAT DER ORGANISATION

8

JAHRE EXTERNER
DATENSCHUTZBEAUFTRAGTER

20+

JAHRE INFRASTRUKTURPRAXIS

DIE KOMBINATION, AN DER ES MEISTENS FEHLT

POSITION

Compliance-Vorhaben scheitern selten am Regelwerk, sondern an der Übersetzung: Der Berater kennt den Katalog, aber nicht die Plattform. Der Engineer kennt die Plattform, aber nicht, was der Prüfer sehen will.

Zwanzig Jahre Infrastruktur- und Netzwerkpraxis bedeuten, dass ich ein Logging-, Segmentierungs- oder Härtings-Control mit dem Verantwortlichen diskutieren kann, statt ihm eine Zeile aus dem Katalog zu schicken und auf Antwort zu warten.

LEISTUNGEN

BSI C5

Gap-Analyse gegen den Kriterienkatalog, Abstimmung von Auslegung und Prüfbedingungen mit dem Prüfer, Mapping gegen bestehende Kontrollsätze, Übersetzung in technische Anforderungen, Nachweisgovernance bis zur Prüfungsreife.

ISO 27001 / 27002

ISMS-Aufbau, Control-Design und -Implementierung, interne Revisionsprozesse, Vorbereitung auf Zertifizierungsaudits.

DSGVO

DSMS-Aufbau, Richtlinienwerk, Verzeichnis von Verarbeitungstätigkeiten, technische und organisatorische Maßnahmen, Schulungen, Auditdokumentation. Acht Jahre als externer Datenschutzbeauftragter.

AUDITSTEUERUNG

Schnittstelle zwischen technischer Organisation und externem Prüfer, Nachweiserhebung und -verwaltung, Enablement der Control Owner, Begleitung der Prüfung.

NIS2, AI ACT

NIS2, CER/KRITIS, EU AI Act: regulatorische Einordnung, Betroffenheitsanalyse, Ableitung des Handlungsbedarfs. Eingearbeitet, ohne bisherige Projektreferenz – das sage ich vorher, nicht im Gespräch.

WIE EIN PROGRAMM BEI MIR LÄUFT

ABLAUF

Gap-Position ermitteln: Was existiert bereits, wo greifen vorhandene Kontrollen, wo ist tatsächlich eine Lücke.

Auslegung mit dem Prüfer klären, bevor gearbeitet wird – der teuerste Fehler ist ein Nachweis, der am Ende nicht akzeptiert wird.

In technische Anforderungen übersetzen, in der Sprache des jeweiligen Teams und mit Begründung.

Control Owner befähigen und führen – Compliance funktioniert nicht durch Zuweisung.

Nachweise governen, eine Schnittstelle zum Prüfer.

Wiederholbar übergeben: die Routinen mitbauen, die das Testat jährlich tragen.

FÜR WEN

ZIELGRUPPEN

Cloud- und Plattformanbieter, die ein C5-Testat brauchen, weil ihre Kunden im öffentlichen Sektor oder in regulierten Branchen danach fragen.

Unternehmen vor einer ISO-27001-Zertifizierung, die feststellen, dass Richtlinien allein nicht ausreichen.

Organisationen mit anstehendem Audit und ohne jemanden, der das Vorhaben bis zum Ergebnis führt.
Unternehmen unter NIS2 oder im Geltungsbereich des EU AI Act, die zuerst wissen müssen, ob und wie stark sie betroffen sind.

ZERTIFIZIERUNGEN

ZERTIFIKATE

Projektmanager (IHK, 2018) · Datenschutzbeauftragter (TÜV, 2023 · DSC/IHK, 2018) · Fachkunde
Datenschutz TTDSG (BvD, 2022) · ITIL4 Foundation

RAHMEN

KONDITIONEN

Verfügbar nach Absprache, Umfang nach Programmzuschnitt. Einsatzgebiet DACH, remote mit Präsenz
zu Prüfungsterminen und kritischen Phasen. Deutsch und Englisch – Prüfungskommunikation in beiden
Sprachen.

KONTAKT

Nennen Sie mir den Rahmen und den Termin. Ich sage Ihnen im ersten Gespräch, ob das realistisch ist – auch wenn die
Antwort unbequem ist.

info@franz.com.de · franz.com.de/vermittler

Vollständiges CV, weitere Referenzen und Konditionen auf Anfrage. Auftraggeber sind in den vollständigen CVs ausgewiesen und im Gespräch
benennbar; in diesem Kurzprofil verzichte ich auf Namensnennung.