Thorsten Franz

Kurzprofil · Informationssicherheit, Compliance & IT-Projektleitung

ISO 27001 · BSI C5 · NIS2 · Cyber Resilience Act · DSGVO — 20+ Jahre Mittelstand und Konzern

+49 1590 6826228 · info@franz.com.de · linkedin.com/in/thorsten-franz
Rottenburg am Neckar, Süßen (Raum Stuttgart) · Deutsch (Muttersprache), Englisch (fließend)

AUF EINEN BLICK

Zielrollen	Informationssicherheitsbeauftragter (ISB) · IT-Compliance Manager · Projektleiter ISO 27001 / NIS2 / CRA · IT-Projektleiter Infrastruktur / ERP · IT-Leiter im Mittelstand
Verfügbar	ab 01.01.2027 – Vorstellungsgespräche ab sofort, auch vor Ort
Vertragsform	Festanstellung (bevorzugt) oder Arbeitnehmerüberlassung; Projektvertrag als Selbständiger möglich
Einsatzgebiet	Großraum Stuttgart, Tübingen/Reutlingen, Göppingen, Ostwürttemberg (Aalen, Heidenheim), Ulm – hybrid, Präsenz nach Bedarf
Unternehmenstyp	Mittelstand 100–2.000 Mitarbeiter – Maschinenbau, Medizintechnik, Energie/Stadtwerke, Gesundheitswesen, öffentliche IT, Systemhäuser
Gehaltsrahmen	Orientierung 80.000–95.000 € Jahresfixum je nach Rolle und Verantwortung; bei Arbeitnehmerüberlassung nach Verrechnungssatz

PROFIL

IT-Projektmanager und Compliance-Praktiker mit über 20 Jahren an der Schnittstelle von Technik, Organisation und Regulatorik. Meine belastbarste Referenz ist ein BSI-C5-Testatvorhaben: Bei STACKIT, der Cloud-Plattform der Schwarz Gruppe, habe ich das erste C5-Programm der Organisation mit KPMG als Prüfer von der Gap-Analyse bis zur Prüfungsreife geführt – Kriterium für Kriterium mit dem Prüfer abgestimmt, gegen ISO 27001/27002 gemappt, in technische Anforderungen übersetzt, Control Owner geführt, Nachweise governt.

Davor Gesamtverantwortung für die IT-Infrastruktur von 14 EU-Großlagern bei Lidl mit drei Neubauten bis zur Vollabnahme, davor fünfzehn Jahre externe IT-Leitung für Mittelständler bis 120 Mitarbeiter und acht Jahre als externer Datenschutzbeauftragter mit eigenständigem ISMS/DSMS-Aufbau. Ausgebildeter Energieelektroniker: Ich kann ein Logging-, Segmentierungs- oder Härtungs-Control mit dem Administrator diskutieren und im selben Termin der Geschäftsführung erklären, warum es jetzt fällig ist.

> *Compliance-Vorhaben scheitern selten am Regelwerk, sondern an der Übersetzung zwischen Katalog, Technik und Prüfer. Genau an dieser Stelle stehe ich.*

1	14	3	8	15+
erstes BSI-C5-Testat der Organisation, KPMG als Prüfer	EU-Großlager in IT-Verantwortung	Neubauten bis zur Vollabnahme geführt	Jahre externer Datenschutzbeauftragter	Jahre externe IT-Leitung im Mittelstand

KERNKOMPETENZEN

Informationssicherheit & Compliance

- BSI C5 – Testatvorhaben mit Big-Four-Prüfer
- ISO 27001 / 27002 – ISMS-Aufbau, Control-Design, interne Revision
- Gap-Analyse, Control-Mapping, Nachweisgovernance
- DSGVO – DSMS, VVT, TOMs, Schulungen, Auditdokumentation
- NIS2 – Betroffenheit, BSI-Registrierung, § 30 BSIG-Maßnahmen
- Cyber Resilience Act – Meldeprozesse, Konformität, SBOM

Projekt- & IT-Leitung

- Projektmanager (IHK), klassisch und agil
- Budget-, Termin- und Qualitätsverantwortung
- RFI/RFP, Ausschreibung, Lieferanten- und Vertragssteuerung
- Gewerkekoordination, Teil- und Vollabnahmen
- Steering Committee, Geschäftsführung, Betriebsrat
- Führung interdisziplinärer Teams, Change-Management

Technische Basis

- Netzwerk und Segmentierung, Firewall, VPN, WLAN
- Serverraum, Verkabelung, WAN-Redundanz, Monitoring
- Proxmox, Private Cloud, Nextcloud, Cloud-Governance
- Härtung, Endpoint-Schutz, Threat Detection, MDM
- ERP-Einführung und -Migration, Schnittstellen, n8n
- Jira, Confluence, ServiceNow, MS Project

WAS ICH MITBRINGE – UND WAS NICHT

Damit Sie das Profil richtig einordnen können, vorab die Punkte, die im Gespräch ohnehin auf den Tisch kommen:

- **Umgesetzt und belegbar:** BSI C5 mit Prüfer, ISO-27001-Kontrollaufbau, ISMS/DSMS als externer DSB, IT-Infrastruktur- und Neubauprojekte im Konzern, ERP-Einführungen im Mittelstand.
- **Eingearbeitet, noch ohne Projektreferenz:** NIS2-Umsetzung, Cyber Resilience Act, EU AI Act, CER/KRITIS. Die Methodik – Betroffenheit, Gap, Maßnahmen, Nachweis – ist dieselbe wie bei C5 und ISO 27001.
- **Kein Hochschulstudium:** Energieelektroniker mit Auszeichnung, Fachhochschulreife, Akademie der Arbeit, zertifizierter Projektmanager (IHK) und Datenschutzbeauftragter (TÜV). Zwanzig Jahre Verantwortung ersetzen bei mir den Abschluss – das muss zum Unternehmen passen.
- **Zertifizierung in Planung:** ISO/IEC 27001 Lead Implementer (TÜV) für Q1/2027 vorgesehen.
- **Werdegang mit Wechseln:** Zwanzig Jahre selbständig, vier Jahre Konzern, zwei Jahre Zypern. Ich kehre bewusst in eine dauerhafte Rolle zurück – nicht als Übergang, sondern weil ich Verantwortung lieber langfristig trage.

STATIONEN

03/2024 – 12/2026	falocon Ltd, Zypern – Business Development & Kundenbetreuung (Teilzeit); daneben freiberufliche Projektberatung DACH
10/2022 – 10/2023	STACKIT (Schwarz IT) – Teamleiter Organisation, Compliance & Interne Revision; erstes BSI-C5-Testat mit KPMG
12/2021 – 09/2022	STACKIT (Schwarz IT) – Senior Prozess- & Organisationsmanager
05/2020 – 11/2021	Schwarz Gruppe / Lidl – Leiter IT-Infrastruktur Lager International, 14 Großlager, 3 Neubauten
07/2019 – 04/2020	Schwarz Gruppe / Lidl & Kaufland – Senior IT Professional Infrastruktur & Filial-Hardware International
04/2003 – 02/2024	FranzX Organisation & IT, Stuttgart – Inhaber: externe IT-Leitung, Projektmanagement, externer DSB (2018–2024)
1992 – 2007	Printor oHG (Mitinhaber) · Gewerkschaft NGG (Politischer Sekretär) · Südmilch AG (Energieelektroniker)

Zertifikate	Projektmanager (IHK, 2018) · Datenschutzbeauftragter (TÜV 2023, DSC 2018) · Fachkunde TTDSG (BvD, 2022) · ITIL4 Foundation, Change Management (Lehrgänge)
Vollständiger Lebenslauf	auf Anfrage sowie unter franz.com.de