Thorsten Franz

Consulting Profile · Information Security, Compliance & IT Project Leadership

ISO 27001 · NIS2 · Cyber Resilience Act · Cloud attestation (BSI C5) · GDPR — 20+ years, mid-market and international group

+49 1590 6826228 · info@franz.com.de · franz.com.de · linkedin.com/in/thorsten-franz
Based in the Stuttgart area, Germany · German (native), English (fluent, working language)

AT A GLANCE

Engagements	ISO 27001 implementation lead · NIS2 readiness and gap closure · Cyber Resilience Act readiness for manufacturers · Cloud attestation / audit programme lead (BSI C5, comparable in rigour to SOC 2) · Interim IT lead · IT infrastructure and ERP project management
Mode	Selected project and interim mandates across the EU – remote-first, on-site by arrangement; direct contract or via agency
Clients	Mid-market manufacturers, cloud and platform providers, healthcare and energy organisations, public bodies – typically 100–2,000 staff
Rates	Day rate on request, depending on scope and duration
Languages	German (native) · English (fluent) – audit communication in both

PROFILE

IT project manager and compliance practitioner with more than 20 years at the intersection of technology, organisation and regulation. My most relevant reference is a cloud attestation programme delivered end-to-end: at STACKIT, the cloud platform of Schwarz Group, I drove the organisation's first BSI C5 attestation with KPMG as external examiner – from gap analysis to audit readiness. C5 is the German federal cloud security standard, comparable in rigour to SOC 2, and it is mapped criterion by criterion against ISO 27001/27002.

That work was as hands-on as a compliance programme actually is: I went through the complete criteria catalogue with the examiner, agreed interpretation and test conditions per control, mapped the criteria against the existing ISO control set, translated each requirement into concrete technical terms for platform and infrastructure teams, enabled the control owners and governed the evidence as the single interface to the auditor.

Before that: full responsibility for the IT infrastructure of 14 large-scale EU warehouses at Lidl, with three new builds delivered to final acceptance; fifteen years as external head of IT for mid-market companies; eight years as external Data Protection Officer building ISMS and DSMS frameworks from policy to training. I trained as an industrial electrician, which means I can discuss a logging, segmentation or hardening control with the engineer rather than hand over a criteria table and wait.

> *Compliance programmes rarely fail on the standard. They fail on translation – between the catalogue, the engineers and the auditor. That is where I stand.*

1st	14	3	8	15+
BSI C5 attestation of the organisation, Big Four examiner	EU large-scale warehouses under IT responsibility	new builds delivered to final acceptance	years external Data Protection Officer	years external head of IT, mid-market

CORE COMPETENCIES

Information security & compliance

- ISO 27001 / 27002 – ISMS build-out, control design, internal audit
- Cloud attestation (BSI C5) – programme lead with Big Four examiner
- Gap analysis, control mapping, evidence governance
- NIS2 – scoping, registration, risk-management measures, incident reporting
- Cyber Resilience Act – vulnerability reporting, conformity preparation, SBOM
- GDPR – DSMS, records of processing, TOMs, training, audit documentation

Project & IT leadership

- Certified project manager (IHK), classic and agile
- Budget, schedule and quality ownership
- RFI/RFP, tendering, vendor and contract management
- Trade coordination, partial and final acceptance
- Steering committee, executive board, works council
- Cross-functional team leadership, change management

Technical foundation

- Networking and segmentation, firewalls, VPN, WLAN
- Server rooms, structured cabling, WAN redundancy, monitoring
- HyperV, Proxmox, Nextcloud, cloud platform governance
- Hardening, endpoint protection, threat detection, MDM
- ERP deployment and migration, interfaces, n8n automation
- Jira, Confluence, ServiceNow, MS Project

HOW A PROGRAMME RUNS WITH ME

- **Establish the gap position.** What exists, where existing controls already apply, where the gap is real. With an ISO 27001 control set in place, the path to C5, NIS2 or CRA conformity is shorter than most assume – if someone does the mapping properly.
- **Agree interpretation with the examiner before work starts.** The most expensive mistake is evidence that is rejected at the end. I agree test conditions and evidence expectations per control up front.
- **Translate into technical requirements.** Not "control X must be implemented", but what the platform, infrastructure or security team actually has to do – in their language, with the reasoning.
- **Enable and lead the control owners.** Compliance does not work by assignment. Owners must understand why something is required, otherwise you get paper instead of effect.
- **Govern the evidence, one interface to the auditor.** I am the single point of contact. That protects your teams from direct requests and the auditor from contradictory answers.
- **Hand over repeatably.** An attestation is not a project with an end but a state that must be confirmed every year. I build the routines that carry it.

TRACK RECORD

10/2022 – 10/2023	STACKIT (Schwarz IT), Germany – Team Lead Organisation, Compliance & Internal Audit; first BSI C5 attestation with KPMG as examiner; ISO 27001 control mechanisms and internal audit routines
12/2021 – 09/2022	STACKIT (Schwarz IT) – Senior Process & Organisation Manager, group-level IT management
05/2020 – 11/2021	Schwarz Group / Lidl – Head of IT Infrastructure, international warehouses: 14 sites (10,000–40,000 m²), 3 new builds (NL/BE) to final acceptance, 99 %+ uptime
07/2019 – 04/2020	Schwarz Group / Lidl & Kaufland – Senior IT Professional, infrastructure and retail hardware, international
2003 – 2024	FranzX Organisation & IT, Stuttgart – owner: external head of IT for mid-market clients (up to 120 staff, up to five parallel mandates), external Data Protection Officer 2018–2024, ERP deployments and migrations
2024 – 2026	falocon Ltd, Cyprus – business development and client management (part-time); independent project consulting across the DACH region
Certifications	Project Manager (IHK, 2018) · Data Protection Officer (TÜV 2023; DSC 2018) · Data protection expertise TTDSG (BvD, 2022) · ITIL4 Foundation, Change Management (courses)
Stated up front	NIS2, Cyber Resilience Act, CER and the EU AI Act are worked in, without a completed project reference yet – same method as C5 and ISO 27001, different catalogue. No university degree: industrial electrician (with distinction) plus the certifications above. Full CV on request and at franz.com.de.