

Thorsten Franz

COMPLIANCE & AUDIT

Advertised as: IT Compliance Manager · Project Manager ISO 27001 / BSI C5 · IT Compliance Consultant

info@franz.com.de · franz.com.de

+357 96017744 · +49 1590 6826228



• AVAILABLE — DACH, CYPRUS, REMOTE & ON SITE — DIRECT CONTRACT

An attestation does not come from documents, but from decisions

On the cloud platform of an international retail group I led the organisation's BSI C5 programme through to audit readiness, with a Big Four audit firm as external auditor – working through the complete criteria catalogue criterion by criterion with the auditor, clarifying interpretation, agreeing test conditions and evidence expectations for each control. The attestation was achieved, after my handover in the final phase.

1st

BSI C5 ATTESTATION FOR THE ORGANISATION

8

YEARS AS EXTERNAL DATA PROTECTION OFFICER

20+

YEARS OF INFRASTRUCTURE PRACTICE

THE COMBINATION THAT IS USUALLY MISSING

POSITION

Compliance programmes rarely fail on the regulation, but on the translation: the consultant knows the catalogue but not the platform. The engineer knows the platform but not what the auditor wants to see. Twenty years of infrastructure and network practice mean I can discuss a logging, segmentation or hardening control with the person responsible, rather than sending them a line from the catalogue and waiting for an answer.

SERVICES

BSI C5

Gap analysis against the criteria catalogue, agreement of interpretation and test conditions with the auditor, mapping against existing control sets, translation into technical requirements, evidence governance through to audit readiness.

ISO 27001 / 27002

ISMS development, control design and implementation, internal audit processes, preparation for certification audits.

GDPR

DSMS development, policy framework, record of processing activities, technical and organisational measures, training, audit documentation. Eight years as an external data protection officer.

AUDIT MANAGEMENT

Interface between the technical organisation and the external auditor, evidence collection and management, enablement of control owners, support during the audit.

NIS2, AI ACT

NIS2, CER/KRITIS, EU AI Act: regulatory assessment, applicability analysis, derivation of what needs to be done. Worked through, without prior project reference – I say that up front, not in the meeting.

HOW A PROGRAMME RUNS WITH ME

SEQUENCE

Establish the gap position: what already exists, where existing controls apply, where there is genuinely a gap.

Clarify interpretation with the auditor before work begins – the most expensive mistake is evidence that is not accepted at the end.

Translate into technical requirements, in the language of the respective team and with the reasoning.

Enable and lead the control owners – compliance does not work by assignment.

Govern the evidence, one interface to the auditor.

Hand over repeatably: build in the routines that carry the attestation year on year.

WHO THIS IS FOR

AUDIENCES

Cloud and platform providers who need a C5 attestation because their customers in the public sector or in regulated industries ask for one.

Companies facing ISO 27001 certification who find that policies alone are not enough.

Organisations with an audit coming up and no one to drive the programme through to the result.

Companies under NIS2 or within the scope of the EU AI Act who first need to know whether and how far they are affected.

CERTIFICATIONS

CERTIFICATES

Project Manager (IHK, 2018) · Data Protection Officer (TÜV, 2023 · DSC/IHK, 2018) · Data Protection Expertise TTDSG (BvD, 2022) · ITIL4 Foundation

FRAMEWORK

TERMS

Available by arrangement, scope according to programme. DACH region, remote with presence at audit dates and critical phases. German and English – audit communication in both languages.

CONTACT

Tell me the framework and the deadline. In a first conversation I will tell you whether that is realistic – even if the answer is uncomfortable.

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

Full CV, further references and terms on request. Clients are identified in the full CVs and can be named in conversation; this short profile refrains from naming them.