

ISO 27001 implementation and audit readiness

For organisations that need ISO/IEC 27001 certification because a customer, tender or regulator has asked for it, and need to know exactly what stands between them and a Stage 2 audit. Delivered by the named principal, ISO/IEC 27001 Senior Lead Implementer and Lead Auditor.

READINESS · 2 TO 3 WEEKS Readiness assessment Establishes ISMS scope and control gaps. Credits in full against a subsequent Sprint. £1,950 from, plus VAT	ASSURANCE · 1 TO 2 WEEKS Pre-certification readiness audit Mock audit ahead of a booked certification audit. £3,500 from, plus VAT	IMPLEMENTATION · TIER 1 ISO 27001 Sprint Focused scope. Single entity, under approximately 50 FTE, one product or service in scope. £14,000 to £22,000, plus VAT
---	---	---

What you receive

- ▶ Gap assessment against Annex A controls with evidence status per control
 - ▶ Information security risk assessment and treatment plan
 - ▶ Mandatory clause 4 to 10 documentation set
 - ▶ Prioritised remediation plan with named owners and dates
- ▶ Statement of Applicability, drafted and justified
 - ▶ ISMS scope statement and context of the organisation
 - ▶ Policy architecture reflecting how the organisation actually operates
 - ▶ Stage 1 and Stage 2 readiness verdict, written plainly

Sprint tiers

TIER	SCOPE	PRICE
Tier 1 · Focused	Single entity, single site or cloud hosted, under approximately 50 FTE, one product in scope, documentation in reasonable shape	£14,000 to £22,000
Tier 2 · Standard	Single entity, 50 to 250 FTE, multiple systems in scope, some existing policy, engineering support available. Most engagements land here	£22,000 to £35,000
Tier 3 · Complex	Multi-entity or multi-site, 250 FTE or above, regulated sector with supervisory expectations, or limited existing documentation	£35,000+

Related engagements

Stage 2 audit defence	Practitioner attendance at the certification audit	Scoped on the diagnostic
ISO 27001 internal audit	Annual clause 9.2 obligation, 1 to 2 weeks	Scoped on the diagnostic
Managed compliance retainer	Keeping certification current without a compliance hire, 12 month minimum	From £1,450/month

Scope boundaries

- Goldline prepares organisations for certification. An accredited certification body issues the certificate. These are separate roles and cannot be performed by the same party.
- Certification body fees, quoted per engagement rather than published, are paid directly to the certification body at cost with no Goldline margin. GRC platform subscriptions likewise.
- Where Goldline has implemented the ISMS it cannot also perform the clause 9.2 internal audit. Independence requires a different party.
- Penetration testing, vulnerability scanning and managed security services are not provided.

Pricing model. Goldline does not bill day rates. Price is fixed at the diagnostic and confirmed in writing before work begins, and does not move afterwards unless scope changes and both parties agree in writing. A day rate rewards a slow engagement. A fixed scope rewards a finished one.