EU GRC Audit-Readiness Blueprint

Who does what in an EU compliance program — monitoring SaaS, accredited auditors and implementation engineering are three different purchases — plus the phased path to an audit-ready ISMS. Brief by OG Technologies EU.

Three jobs, three vendors

Layer	Example vendors	What they do	What they cannot do
Monitoring SaaS	Vanta, Drata	Continuous control monitoring, evidence collection	Write your policies, risk treatment or SoA; US-cloud first; limited DORA/EN 18286 depth
Audit & certification bodies	Coalfire, A-LIGN, TUV	Accredited ISO/SOC 2 attestation (ANAB/UKAS)	Build the system they audit — independence rules forbid it
Implementation engineering	OG Technologies EU	Builds ISMS/QMS/AIMS, living SoA, DORA register tooling, evidence workflows	Issue the attestation — that is the auditor's job

Phased path to audit readiness

Phase	Work	Output
Weeks 1–2	Gap & readiness sprint: scope, asset inventory, control-by-control status	Written gap report + remediation roadmap + living SoA structure
Weeks 3–8	Management-system build: policies, registers, evidence workflows, DORA register of information	Working ISMS/AIMS integrated across ISO 9001 + 27001 + 42001
Weeks 9–12	Internal audit + pre-audit rehearsal; fix nonconformities	Evidence pack the accredited auditor examines

The Annex SL multiplier

Fact
~65% of ISO 9001/27001/42001 clauses share the Annex SL core — one integrated management system beats three parallel spreadsheets.
EN 18286 gives the EU AI Act its QMS backbone — layer it onto the same document control, internal audit and management review.