TECHNICAL SHEET · 2026

ISOPILOT Technical Sheet

Architecture, capabilities, security, AI Governance, integrations and operating model - 2026 commercial release.

AI-powered Governance, Risk & Compliance Operating System

ISO + GDPR + NIS2 + MOG 231 + Continuous Compliance + Evidence Intelligence + Audit + Risk/CAPA + AI Governance + Integrations + Automation

Product	Validation
UESE ITALIA S.p.A.	Dozens of Senior Specialist consultants with international experience.

isopilot.it · uese.eu

Compliance & Governance Operating System

ISOPILOT combines specialist workspaces with a shared GRC layer while keeping tenants, projects, authoritative sources and professional decisions under control.

Control Center	Continuous Monitoring
Compliance score, framework readiness, missing evidence, risks, audits, NC/CAPA, deadlines.	Findings, owners, operational targets, escalation, remediation and reopening history.

Evidence Intelligence	Audit Readiness
Type, fingerprint, reliability, validity, duplicate/obsolete detection and cross-framework mapping.	0-100 readiness, requirement-document-evidence-owner matrix, Simulate Audit, Audit Copilot.

Risk & CAPA	Document Consistency
Inherent/residual risk, treatment, heatmap, root cause, 5 Whys, Ishikawa, effectiveness.	Change events, impact preview, protected documents and governed Smart Update.

- Regulatory Change Intelligence: institutional sources, fingerprints, qualification and impact analysis.
- AI Compliance Agents: 11 specialist agents grounded in tenant data.
- Knowledge Graph: natural-language search with internal citations and navigable relationships.

Specialist frameworks, shared data where appropriate

ISO / SGSI	GDPR Privacy Governance
ISO systems; for 27001: RACI, scope, Asset Register, Risk Register, Annex A, SoA, suppliers, incidents and audits.	RoPA, legal bases, LIA, DPIA, Art. 28, DSAR, breaches, transfers/TIA, retention and security measures.

NIS2 Cybersecurity Governance	MOG 231 Advanced Governance
Scope, governance, measures, assets, risk, supply chain, IAM, incidents, BCP/DR, evidence and governed documentation.	Offence risk assessment, sensitive processes, General/Special Parts, protocols, Supervisory Body, flows, whistleblowing and training.

Cross-framework layer

- Evidence once, comply many: confirmed evidence can support multiple requirements.
- Risk once, govern many: one risk can be linked across frameworks without logical duplication.
- Multi-Standard Master Project: integrated programme for multi-framework organizations.

Explainable, auditable, human-in-the-loop AI

No Hallucination Policy	Epistemic status
People, roles, dates, evidence, regulations and certifications must not be invented.	CONFIRMED / INFERENCE / TO VALIDATE with sources and confidence where available.

AI Governance Register	Natural Language Search
User, tenant, operation, source, input/output fingerprints, provider/model when exposed and human review.	Operational questions on real tenant data with internal source codes.

Specialist agents

ISO Compliance · Audit · Evidence · Risk · Document · Regulatory Change · MOG 231 · GDPR · NIS2 · SGSI / ISO 27001 · AI Act / ISO 42001

Portfolio, Board, onboarding and roadmap

Consultant Workspace 2.0	Executive Board Dashboard
Client portfolio, issues, readiness, documents requiring approval and Client Health Score.	Compliance level, top risks, audit, NC/CAPA, trends, deadlines and Executive Compliance Report PDF.

Intelligent Onboarding	Certification Roadmap
Wizard for organization, sector, processes, frameworks, roles, IT, suppliers and initial configuration proposal.	Where we are → what is missing → what to do → who → when, without promising certification.

Integration Hub & Automation

- Signed inbound HMAC-SHA256 webhook and Generic HTTPS REST with SSRF protection.
- Evidence Inbox with review before content is used as evidence.
- IF/THEN Automation Builder for tasks, notifications and webhooks; no automatic critical closures/approvals.

Security and accountability as product requirements

Tenant isolation	Identity & access
Server-side company scope and cross-tenant access protection.	Roles, segregation, 2FA where configured, Trial Security and IP/CIDR blocklists.

Application security	Auditability
CSRF, XSS/escaping, upload/file access controls and integration security by module.	Sensitive operations, reviews, owners, targets and changes preserve evidence and history.

Produced and distributed by UESE ITALIA S.p.A.

The platform is produced and distributed by UESE ITALIA S.p.A., a leading Italian company in management systems, compliance and cybersecurity services, and is developed and validated with contributions from dozens of Senior Specialist consultants with international experience. Professional outputs remain subject to correct data, requirement applicability and final validation.

- https://isopilot.it/
- https://isopilot.it/en/enterprise
- https://isopilot.it/en/compare
- sales@uese.it
- +39 02 5656 8416
- https://uese.eu/