SCHEDA TECNICA · 2026

Scheda tecnica ISOPILOT

Architettura, capability, sicurezza, AI Governance, integrazioni e modello operativo - Release commerciale 2026.

AI-powered Governance, Risk & Compliance Operating System

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

Prodotto	Validazione
UESE ITALIA S.p.A.	Decine di consulenti Senior Specialist con esperienza internazionale.

isopilot.it · uese.eu

Compliance & Governance Operating System

ISOPILOT combina workspace specialistici e un livello GRC condiviso, mantenendo tenant, progetti, fonti autorevoli e decisioni professionali sotto controllo.

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: fonti istituzionali, fingerprint, qualifica e impact analysis.
- AI Compliance Agents: 11 agenti specialistici grounded sui dati del tenant.
- Knowledge Graph: ricerca naturale con citazioni interne e relazioni navigabili.

Framework specialistici, dati condivisi quando ha senso

ISO / SGSI	GDPR Privacy Governance
Sistemi ISO; per 27001: RACI, scope, Asset Register, Risk Register, Annex A, SoA, fornitori, incidenti, audit.	RoPA, basi giuridiche, LIA, DPIA, Art. 28, DSAR, breach, trasferimenti/TIA, retention, misure di sicurezza.

NIS2 Cybersecurity Governance	MOG 231 Advanced Governance
Perimetro, governance, misure, asset, rischio, supply chain, IAM, incidenti, BCP/DR, evidenze e fascicolo documentale.	Risk assessment reati, processi sensibili, Parte Generale/Speciali, protocolli, OdV, flussi, whistleblowing, formazione.

Cross-framework layer

- Evidence once, comply many: una evidenza confermata può supportare più requisiti.
- Risk once, govern many: un rischio può essere collegato a più framework senza duplicazione logica.
- Multi-Standard Master Project: programma integrato per organizzazioni con più schemi.

AI spiegabile, auditabile e human-in-the-loop

No Hallucination Policy	Epistemic status
Persone, ruoli, date, evidenze, norme e certificazioni non devono essere inventate.	CONFERMATO / INFERENZA / DA VALIDARE con fonti e confidence quando disponibili.

AI Governance Register	Natural Language Search
Utente, tenant, operazione, fonte, fingerprint input/output, provider/modello quando esposti, review umana.	Domande operative sui dati reali del tenant con codici sorgente interni.

Agenti specialistici

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

Portfolio, Board, onboarding e roadmap

Consultant Workspace 2.0	Executive Board Dashboard
Portfolio clienti, criticità, readiness, documenti da approvare e Client Health Score.	Compliance level, top risks, audit, NC/CAPA, trends, deadlines and Executive Compliance Report PDF.

Intelligent Onboarding	Certification Roadmap
Wizard organizzazione, settore, processi, schemi, ruoli, IT, fornitori e proposta iniziale da confermare.	Dove siamo → cosa manca → cosa fare → chi → quando, senza promettere la certificazione.

Integration Hub & Automation

- Signed Webhook inbound HMAC-SHA256 e Generic HTTPS REST con protezione SSRF.
- Evidence Inbox con review prima di usare il contenuto come prova.
- Automation Builder IF/THEN per task, notifiche e webhook; niente chiusure/approvazioni critiche automatiche.

Sicurezza e responsabilità come requisiti di prodotto

Tenant isolation	Identity & access
Scope azienda server-side e protezione da accessi cross-tenant.	Ruoli, segregazione, 2FA dove configurata, Trial Security e blocklist IP/CIDR.

Application security	Auditability
CSRF, XSS/escaping, upload/file access controls e sicurezza integrazioni secondo modulo.	Operazioni sensibili, review, owner, target e variazioni mantengono evidenze e storico.

Prodotto e distribuito da UESE ITALIA S.p.A.

La piattaforma è sviluppata e validata con il contributo di decine di consulenti Senior Specialist con esperienza internazionale. Gli output professionali restano soggetti a correttezza dei dati, applicabilità dei requisiti e validazione finale.

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