

ROLE MANUAL · EN

Superadmin Manual

Superadmin - ISOPILOT 2026

AI-powered Governance, Risk & Compliance Operating System

ISO + GDPR + NIS2 + MOG 231 + Evidence Intelligence + Risk Intelligence + Audit Intelligence + AI Governance + Integrations + Automation

isopilot.it | UESE ITALIA S.p.A.

Role objective

This manual describes the essential operating path for using ISOPILOT within your authorization level.

- Govern plans, entitlements, companies, tenants and trial security.
- Manage IP/CIDR blocklists and suspensions without deleting data.
- Manage Regulatory Change sources and qualification of changes.
- Supervise integrations, automation and AI Governance at platform level.
- Preserve tenant isolation, audit trails, backups and release compatibility.

Daily operating flow

Activities follow a logic of evidence, ownership, review and traceability.

- 1. Open the Control Center or assigned project.
- 2. Review findings, tasks, deadlines and documents requiring review.
- 3. Work on the authoritative source: evidence, risk, audit, document or CAPA.
- 4. Use AI and automation as support, not as a decision-making shortcut.
- 5. Complete with review, rationale and audit trail where required.

Key modules

Actual availability depends on plan, role, entitlement and project.

- Compliance Control Center / Continuous Compliance
- Evidence Intelligence / Compliance Search / AI Compliance Agents
- Audit Readiness / Risk & CAPA / Document Consistency
- Regulatory Change / Security & AI Governance
- Consultant Workspace / Board / Onboarding / Roadmap / Integration / Automation

Security and support

Do not share credentials, approve unverified items or upload unnecessary data. When in doubt, use support or your company contact.

- 2FA where enabled/configured.
- Tenant isolation and server-side permissions.
- Human review for AI outputs and material changes.
- Support: <https://isopilot.it/support>
- Manuals: <https://isopilot.it/en/manuals>

Open ISOPILOT