GOVERN AI - DELIVERING SECURITY & RISK ASSURANCE

RiskOpsAI™ is a Unified GRC platform that provides streamlined governance, delivering continuous control monitoring, continuous compliance and continuous risk assessment. We provide advanced red teaming of the AI pipeline for security, compliance and risk assurance. By automating the risk and compliance lifecycle, our proactive and continuous assessments identify operational weaknesses, security flaws and data and control gaps across AI models and systems before problems arise. Visit: https://www.riskopsai.com

USE CASE

Continuous and Unified Compliance - Test Once. Comply with Many.

A proactive, AI-native approach to compliance that replaces fragmented, framework-by-framework programs with a single unified control architecture — reducing cost, effort, and regulatory exposure across the enterprise.

THE CHALLENGE

- Fortune 1000/2000 enterprises face multiple overlapping compliance mandates simultaneously — with separate teams, tools, and budgets per framework
- Separate control libraries per framework create duplication, redundancy, and unmanageable maintenance overhead
- Point-in-time, quarterly attestation cycles leave compliance posture blind between audits
- Evidence collected for one framework cannot be reused — every audit restarts from scratch
- No weighted visibility into how a control failure impacts multiple frameworks simultaneously
- Regulatory change tracking is manual, slow, and error-prone across 200+ mandates
- Compliance posture is measured at the enterprise level only — no drill-down by product, geography, or business unit
- Risk quantification is limited to H/M/L heat maps — no dollar-based exposure for boards and CXOs

RiskOpsAI™ SOLUTION

- Our Common Control Collection across 70,000+ controls — one architecture behind every mandate, eliminating duplication
- Test once, comply with many — automated crosswalk across 230+ frameworks including SOC 2, ISO 27001, NIST CSF, GDPR, HIPAA, PCI DSS, CMMC, FedRAMP, DORA, NIS2, and 220+ more
- Always-on, real-time control monitoring — replaces quarterly attestation cycles with continuous compliance posture
- Evidence collected once is automatically applied to every applicable framework — dramatically reducing audit preparation cost
- Cause-and-effect analytics map each control's weighted impact across every framework with financial quantification
- AI-automated regulatory change monitoring — changes mapped to internal policies and controls without manual effort
- Full hierarchical drill-down by product line, geography, and business unit — precise, accountable remediation
- ROAR® Automation Engine — automates risk orchestration, assessment review, risk register maintenance, and remediation workflows

70,000+	230+	1×	Always-on
Unified controls in ourCommon Control Collection	Compliance frameworks mapped and crosswalked	Test once — evidence reused across all mapped frameworks	Real-time control monitoring, not point-in-time audits

DIFFERENTIATED VALUE PROPOSITION

01 — Common Control Collection — 70,000+ Controls, One Architecture

Rather than maintaining separate control libraries per framework, RiskOpsAI™ ingests all data and controls into a single Common Control Collection. Every regulation, every standard, every mandate maps back to one master control set — eliminating duplication, reducing maintenance overhead, and giving compliance teams a single source of truth across the entire enterprise.

Key benefits: 70,000+ controls · One control library · All frameworks unified · No duplication

02 — Test Once, Comply with Many — Automated Crosswalk Across 230+ Frameworks

RiskOpsAI™'s ready-to-go crosswalk engine maps tested controls simultaneously across SOC 2, ISO 27001, NIST CSF, GDPR, HIPAA, PCI DSS, CMMC, and 220+ more. Evidence collected once is automatically applied to every applicable framework — dramatically reducing the cost, time, and resource effort of compliance testing cycles.

Frameworks include: SOC 2 · ISO 27001 · NIST CSF · GDPR · HIPAA · PCI DSS 4.0 · CMMC 2.0 · DORA · NIS2 · FedRAMP · and 220+ more

03 — Full Drill-Down — By Product, Geography, and Business Unit

Compliance posture is never a single number. RiskOpsAI™ delivers a full hierarchical drill-down so leadership can see compliance status at the enterprise level, then step into any product line, geographic region, or business unit to understand exactly where gaps exist and why — enabling precise, accountable remediation rather than blanket responses.

- **By geography:** EMEA (GDPR, NIS2, DORA), APAC (MAS TRM, PDPA), Americas (SOX, CCPA, FedRAMP) — see where you're exposed by jurisdiction.
- **By product line:** Map compliance coverage to each product or service offering — understand which products carry the most regulatory exposure and where control gaps exist.
- **By business unit:** Isolate compliance posture by division, subsidiary, or function — giving business unit owners accountability and risk teams precision in remediation planning.

04 — Cause-and-Effect Analytics — Know Which Controls Drive Which Frameworks

Most GRC platforms tell you if a control passes or fails. RiskOpsAI™ tells you what it means. Our cause-and-effect analytics engine maps every control's weighted impact across every framework — so risk teams can see that a single access control may be 90% effective for NIST CSF but only 10% effective for ISO 27001. This enables prioritized remediation investment, not guesswork.

Example — one access control, tested once, weighted across frameworks:

Framework	Control Effectiveness
NIST CSF 2.0 — Identity & Access Mgmt	**90%**
SOC 2 Type II — Logical access controls	**78%**

PCI DSS 4.0 — Requirement 7	**65%**
HIPAA — Access control safeguards	**52%**
ISO 27001:2022 — A.9 Access control	**10%**

Key benefits: Weighted control impact · Cross-framework analytics · Prioritized remediation · Financial quantification

CAPABILITY COMPARISON — LEGACY GRC vs RISKOPSAI™

Capability	Legacy GRC	RiskOpsAI™
Control architecture	Separate library per framework	**Common Control Collection — 70K+ controls**
Testing approach	Test separately per framework	**Test once, comply with 230+ frameworks**
Compliance monitoring	Point-in-time, quarterly cycles	**Always-on, real-time continuous monitoring**
Cause-and-effect analytics	Pass / fail — no weighted impact	**Weighted control impact per framework with financial quantification**
Drill-down granularity	Enterprise-level only	**By product, geography, and business unit**
Regulatory change	Manual tracking and mapping	**AI-automated regulatory change monitoring and crosswalk**
Quantification	H / M / L heat maps	**Dollar-based financial risk impact for the C-suite and board**

INSIDE THE PLATFORM — KEY CAPABILITIES

- **Data Aggregation —** Ingests structured and unstructured data from across the enterprise to build a comprehensive, unified compliance profile.
- **Predictive Risk Management —** AI models analyze diverse datasets to identify emerging compliance risks and recommend proactive mitigation strategies before exposure occurs.
- **ROAR® Automation Engine —** Risk Orchestration Automation Responses® automates assessment review, risk register maintenance, and remediation workflows — reducing manual effort and regulatory exposure.
- **Regulatory Change Management —** AI monitors regulatory updates continuously, mapping changes to internal policies and controls to maintain posture without manual effort.
- **Data Quality Governance —** Data quality measured by framework coverage — automatically moderated to ensure AI models operate on accurate, high-integrity inputs.
- **Continuous Learning —** AI/ML models train on your data over time — adapting to your regulatory environment and improving decisioning precision as your posture evolves.

WHAT SETS US APART

- **Competitive Differentiation —** Customized from day one to quantify, automate, and govern AI risk across the three lines of defense — not a retrofit on legacy GRC.

- **Dual-Play Approach —** Bottom-up operational risk + top-down governance — not one or the other.
- **Threat-Likeliness Vector™ —** Multi-dimensional matrix minimizing subjectivity — residual risk in financial terms.
- **Financial Risk Quantification —** Dollar-based impacts for CXOs, C-Suite & Board — not qualitative heat maps.
- **Continuous Compliance —** Real-time control monitoring across 230+ frameworks — not point-in-time.
- **Native Framework Mapping —** Cross-walk regulatory requirements — not isolated modules.
- **Three Lines of Defense —** ERM dashboards, drill-downs, remediation — the Autonomous Risk Register is central.

Capability	Legacy GRC	RiskOpsAI™
Approach	Top-down only	**Dual play**
Controls	Declared states	**Continuous matrix**
Quantification	H / M / L	**Financial ($)**
Compliance	Evidence gathering	**Real-time · 230+**
Reporting	Quarterly certs	**Always-on ERM**

GO-TO-MARKET TOGETHER

Flexible Partner Models

We go to market with our partners — solving client problems together. Two proven engagement models to accelerate your AI governance practice and create recurring revenue.

WHITE LABEL

Your Brand, Our Platform

- Full platform white-labeling with your brand identity
- Dedicated instance per partner or per client
- Custom framework & control library configuration
- Partner-managed client onboarding & support
- Recurring SaaS revenue share model
- 24/7 support from RiskOpsAI™

JOINT GO-TO-MARKET

Stronger Together, Co-Branded

- Co-branded solution positioning & marketing
- Joint sales enablement & proposal support
- Partner leads strategy; RiskOpsAI™ deploys platform
- Shared delivery: Assess → Design → Deploy → Monitor
- Executive dashboards & board-ready reporting

Both models include a data ingestion readiness assessment and IT partnership framework to ensure the client's data architecture supports the governance capabilities — from batch feeds for baseline profiling to real-time streaming for agentic AI monitoring.

AI GOVERNANCE ACCELERATOR

Every partner engagement includes RiskOpsAI™'s AI Security & Risk Assurance module — pre-built with 10 assurance dimensions (comprising emerging AI regulations and standards) enabling partners to offer board-ready AI governance from day one.