

GOVERNANCE, RISK & COMPLIANCE

ScaleRisk

An AI-driven enterprise risk and compliance platform. One system of record for risk, controls, policies, evidence and incidents.

ONE SYSTEM OF RECORD

UNIFIED COMPLIANCE

ACCOUNTABLE AI

SOVEREIGN

01 THE FRICTION – WHERE GRC PROGRAMMES BREAK DOWN

Wrong altitude

Leaders drown in raw detail; operators lack direction on what to do next.

Duplicated evidence

The same artifact re-collected for every framework it satisfies.

Scattered risk

Risk sits across spreadsheets and team silos, with no common owner or score.

Policy drift

What is written stops matching what is practised, and what can be proven.

Audit fire-drills

Coverage reassembled by hand, under deadline, every cycle.

No single truth

Risk counts and control status disagree depending on which tool you open.

02 THE OPERATING MODEL

A modern GRC programme runs on four principles

One system of record

Risk, controls, policies, evidence and incidents in one place, related to each other.

Capture once, reuse everywhere

Mapped to every control it satisfies: collected once, credited many times.

The event is the audit record

Every material action logged immutably by default. Always audit-ready.

Right signal, right altitude

Leaders see direction, managers see what is overdue, operators see their queue.

03

THE ANSWER, STRUGGLE BY STRUGGLE

THE STRUGGLE	WHAT SCALERISK DOES
Leaders buried in detail	Role-tailored surfaces — board-ready signal up, task queues down.
Policies drift from practice	Policies linked to the controls they enforce, with acknowledgement tracking.
Evidence re-collected per framework	Common-controls repository — upload once, fan out to every framework it satisfies.
Audit assembled under deadline	Audit packages inherit already-approved evidence and export for the auditor.
Risk tracked in spreadsheets	Enterprise risk register with named owners, scoring and treatment status in one live view.
Vendor risk assessed once, then forgotten	Third-party assessments with ongoing monitoring, tied to the same controls and evidence.

04

THE PLATFORM CAPABILITIES

Risks Register with owner, inherent and residual score with trend, annualised loss expectancy and treatment status.	Policies Versioned and linked to the controls they enforce, with acknowledgement tracking and review cycles.	Compliance Coverage and gaps per framework, status down to the requirement, policy coverage per control, and evidence validated, expiry-tracked and exported as an audit package.
Third-party risk Onboarding assessments and ongoing vendor monitoring, tied to the same controls and evidence.	Reports Assessments on NIST SP 800-30, ISO 27005, ATT&CK or BIA methods, plus audit trail and action items.	Strategy Roadmap, charter and budget for the security leader, with board decks generated from live posture.

FRAMEWORKS IN LIBRARY

SAMA · NCA ECC · CBUAE ISR · Oman NIAF · SEBI · ISO 27001 · NIST CSF · PCI DSS · SOC 2 · GDPR · DORA

05

ACCOUNTABLE AI

The AI proposes, your people decide

Cross-framework mapping, policy gap analysis and treatment-plan drafting arrive as suggestions. A named owner accepts, amends or rejects with reason, and the record keeps the model version, source, reviewer, decision and timestamp.

No control auto-closes · no evidence auto-approves · your data never trains our models

06

WHERE IT RUNS

Residency where your regulator says

- IN-REGION SAAS

PRIVATE CLOUD

AIR-GAPPED

A separate data plane per customer, customer-managed keys, SSO and granular roles. UAE and India regions, or fully isolated for critical national infrastructure.

DIFFERENTIATORS

- Compliance coverage and gaps in one view

■ Air-gapped for critical infrastructure

■ MEA regimes native

■ Deployed in weeks