OFFLOAD SECURITY

Compliance & Risk Management (GRC)

Module Whitepaper

Compliance that reflects technical reality — controls, risks, evidence, and BIA connected to live findings

Version 1.0 · July 2026 · Classification: Customer-Shareable

1. Overview

The GRC module unifies compliance posture, enterprise risk management, and business impact analysis — and, unlike standalone GRC tools, wires them to the platform's live technical findings so dashboards, risk scores, and audit evidence reflect the actual state of the environment.

2. Key Capabilities

- Framework assessments and control posture: ISO 27001, SOC 2, SCF, and additional frameworks, with per-team control state.
- Technical findings mapped to compliance controls — a failed control is backed by the findings that fail it.
- Enterprise risk register with composite scoring: CVSS, EPSS, KEV, and business context.
- Cross-module correlators: attack-path toxic combinations, failed compliance controls, and BIA criticality all feed risk scoring.
- Treatment plans with SLA escalation; risks auto-close when their underlying findings resolve.
- Business Impact Analysis: RTO/RPO and financial impact per business process, correlated into risk prioritization.
- Security-questionnaire automation: AI-assisted answering of customer and vendor questionnaires from an approved knowledge base with evidence linkage.
- Automated audit, customer, and management reporting.

3. How It Works

A dedicated integration layer connects the GRC modules: correlators bridge compliance posture, attack-path analysis, and BIA into risk scoring without duplicating any module's data. Failed controls mint risks; resolved findings close them; every transition is observable and audited.

Assessments combine automated control evaluation (where technical evidence exists on-platform) with guided manual attestation, producing framework-mapped posture with a defensible evidence trail.

4. Data Handling & Security

Aspect	How it is handled
Credential protection	All connection credentials are encrypted at rest with Fernet authenticated encryption (AES-128-CBC + HMAC), decrypted in memory only at the moment of use, and never returned by APIs.
Tenant isolation	Every record is scoped to the owning team; all reads and writes filter on the tenant identifier, enforced by database indexes.
Retention & deletion	Results are subject to configurable retention windows; data can be hard-deleted

Aspect	How it is handled
	per scan and is removed by the tenant-offboarding cascade.
Deployment	Available as SaaS or fully self-hosted / on-premises — in the on-premises model no security data leaves your environment.

5. One Platform, One Risk View

GRC consumes every other module's findings and produces the executive layer above them: compliance dashboards, the risk register, treatment workflows, and generated reports — one system where the scan result and the audit answer trace to the same record.