SentinelUnity
GRC PLATFORM

RISK MANAGEMENT

Every risk, scored your way, measured against the appetite the board set.

Enterprise, operational, IT, cyber and third-party risk in one register, on one methodology — with appetite, indicators and escalation that act on their own instead of waiting for the quarterly review.

ENTERPRISE OPERATIONAL IT & CYBER THIRD-PARTY INDICATORS

Software for Enterprise Risk Teams

Your taxonomy, your matrices, your formulas. SentinelUnity runs the methodology you already defend to the board, then compares every score to appetite, escalates on its own, and explains how each number was reached.

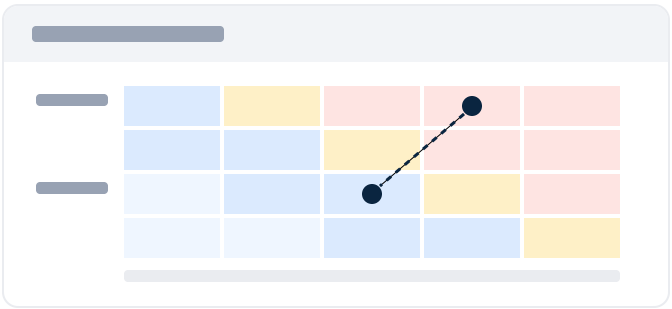
APPLICATIONS

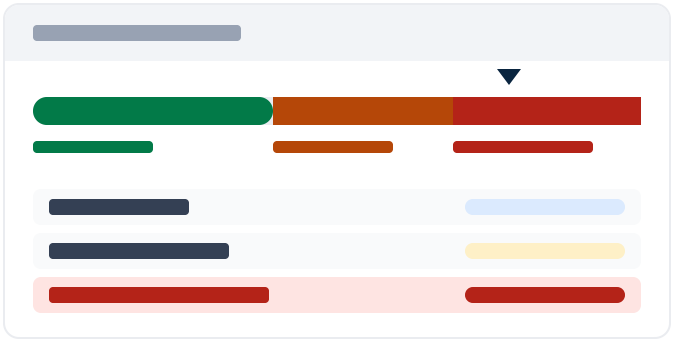
- Risk Register
- Methodology & Matrices
- Appetite & Tolerance
- Treatment & Acceptance
- Escalation
- Board Reporting

Your methodology, not ours

Versioned taxonomies, matrices, severity bands and scoring formulas are configuration, not code. Score on a matrix, or quantitatively with frequency and magnitude distributions and scenarios.

- Inherent, residual and target scoring
- Every score explains its factors





Appetite that acts

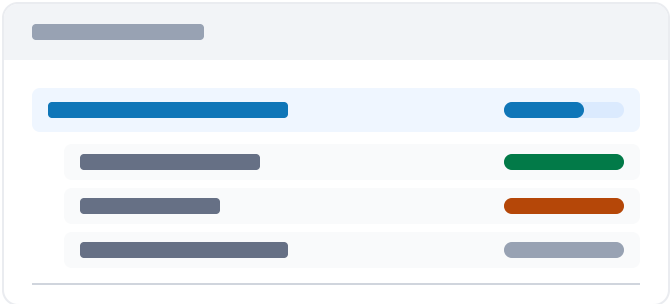
Define appetite and tolerance per category, entity or objective. Each risk lands within appetite, within tolerance, above tolerance or outside appetite — and a breach runs the action you chose.

- Notify, escalate, mandate treatment, board
- Escalates overdue treatment, lapsed acceptance

Treatment & Acceptance

Treatment plans hold actions with owners, targets and the controls they rely on; control effectiveness feeds the residual score. Acceptances expire; reviews run on a cadence.

- Named owners, confidential-risk visibility
- Board pack export with trend and history



Software for Operational, IT & Cyber Risk

Operational, IT and cyber risk are programs on the same register, each with its own context: the self-assessment behind an operational risk, the service behind an IT risk, the threat, vulnerability and asset behind a cyber one.

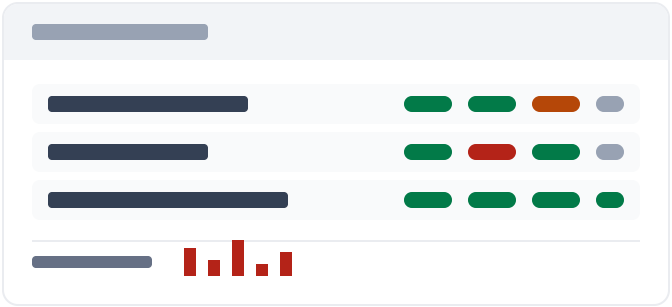
APPLICATIONS

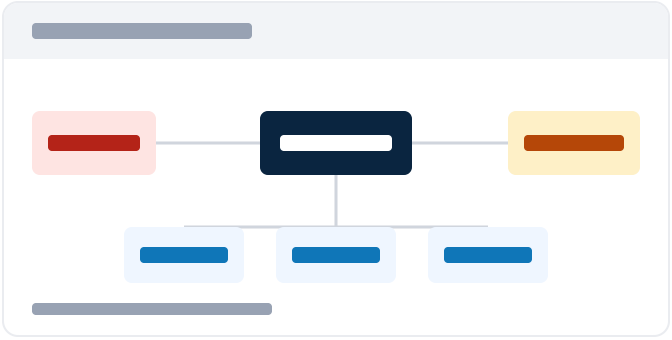
- RCSA Cycles
- Loss Events
- IT Service Risk
- Threats & Vulnerabilities
- Security Events & Automation
- Assets

RCSA & Loss Events

Run control self-assessment cycles by department: each entry scores the risk, assesses its controls and feeds the register. Loss events keep their later adjustments, so actual losses sit beside estimates.

- Cycle-based self-assessment with sign-off
- Loss history that informs reassessment





IT & Cyber Risk

A threat and vulnerability catalogue links to the assets it affects. Security events arrive from your tooling, and automation rules decide when one should raise a risk, rescore it or open remediation with an SLA.

- Service dependency view for IT risk
- Field assessment campaigns to the front line

Assets

A structured asset register — categories, types, environments, data classification, valuation — with relationships between assets and links to the risks, controls, policies and findings on each.

- Asset requests, approvals and lifecycle events
- Assignments and consumers per asset

Software for Third-Party Risk & Indicators

A third party is a risk you have contracted for. SentinelUnity tiers every vendor by the factors you weight, keeps contract and obligations beside the assessment, and watches the whole register through indicators that escalate on breach.

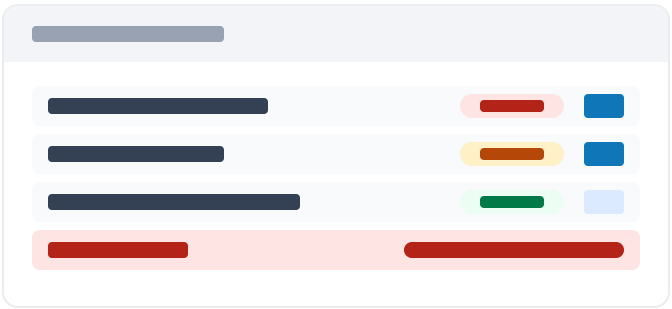
APPLICATIONS

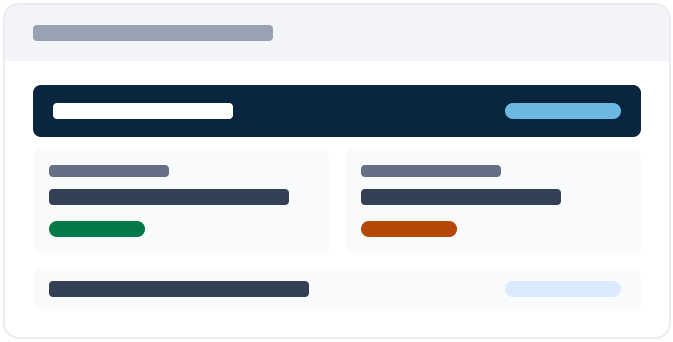
- Third & Fourth Parties
- Engagements & Contracts
- Due Diligence
- Tiering & Knockouts
- Issues
- Key Risk Indicators

Tiering & Due Diligence

Inherent-risk factors you weight decide the tier; knockout rules stop a vendor regardless of score. Each tier sets the questionnaire depth and review schedule, and due-diligence requests are tracked to a decision.

- Scoring bands and control domains per profile
- Fourth parties and dependency links





Engagements, Contracts & Issues

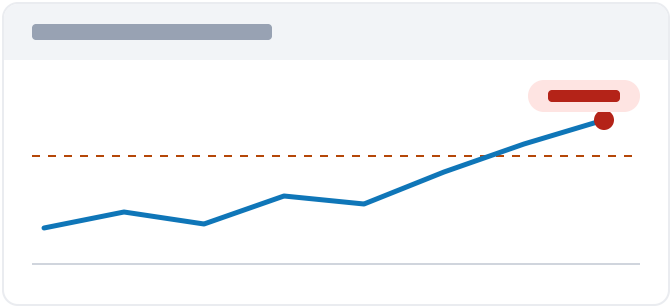
Each engagement names the services and assets a vendor touches. Contracts carry obligations, a review and approval trail and status history; issues raised against a vendor are tracked to closure alongside its risk.

- Contract obligations with review approvals
- Vendor lifecycle history end to end

Key Risk Indicators

Indicators sit on any program with thresholds and a reading history. A breach is an escalation reason in its own right, so the review opens before anyone has to notice the trend.

- Readings, thresholds and breach history
- Program dashboards and a global overview



One platform underneath every risk program

Enterprise, operational, IT, cyber and third-party risk are programs on one register, sharing people, controls, assets and the workflow engine — and they sit beside strategy, compliance and policy on the same platform.

WORKFLOW DESIGNER

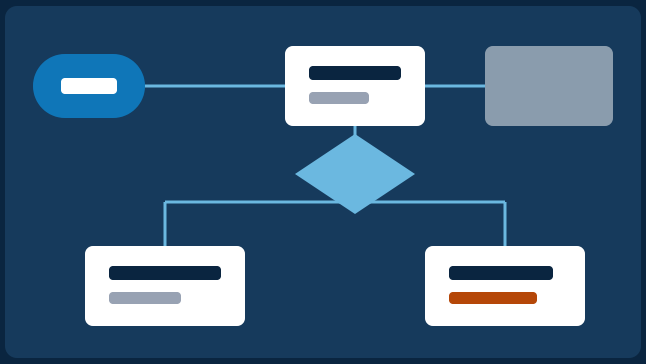
No code — but real logic.

Risks move through a lifecycle you can reshape — identified, assessed, in treatment, accepted, closed — with structured conditions, scheduled and date-field triggers, escalation ladders and role-gated transitions, drawn as a flowchart and run by the engine.

Flow templates per module

Scheduled & date triggers

Escalation ladders



Tenant isolation at the database

Database row-level security enforces company boundaries below the application, on every query, for every module.

Roles and separation of duties

Records are owned by named people. Object-level scoping, SoD pairs and role-gated transitions decide who may move what.

Linked records

Any record links to any other, in both directions. A risk's page shows its assets, controls, findings, objectives, third parties and the threats behind it.

Dashboards and reports

Program dashboards, trend views and a board pack export; generated reports stored alongside the records they cite.

Import, custom fields, languages

Bulk data import, custom fields on any module, notifications, full-text search and localisation for multilingual teams.

Deploy your way

Single-tenant on your own infrastructure or multi-tenant SaaS. Packaged as Startup, Mid-Market and Enterprise tiers.

ENTERPRISE RISK

Risk Register
Methodology & Matrices
Appetite & Tolerance
Treatment & Acceptance
Escalation
Board Reporting

OPERATIONAL, IT & CYBER

RCSA Cycles
Loss Events
IT Service Risk
Threats & Vulnerabilities
Security Events & Automation
Assets

THIRD-PARTY & INDICATORS

Third & Fourth Parties
Engagements & Contracts
Due Diligence
Tiering & Knockouts
Issues
Key Risk Indicators

PLATFORM

Workflow Designer
Linked Records
Access Control & SoD
Dashboards & Reports
Data Import & Custom Fields
Localisation

ABOUT SENTINELUNITY

SentinelUnity is a governance, risk and compliance platform built on a single data model, so strategy, risk, control and evidence are one set of records rather than four. It runs as single-tenant software on your infrastructure or as multi-tenant SaaS.

SEE IT IN ACTION

Ask for a walkthrough of a fully populated demonstration environment — a live register with appetite, indicators, treatments and escalations already in motion.

www.sentinelunity.com
support@sentinelunity.com