



SentinelUnity
GRC PLATFORM

THIRD-PARTY RISK

Every vendor tiered, assessed, contracted and watched — for as long as you depend on them.

Third parties, engagements, contracts, assessments and fourth-party exposure on one record set — so the risk of a vendor is read from what they touch, what they signed and how they scored, not from a spreadsheet tab.

ONBOARDING

TIERING

DUE DILIGENCE

CONTRACTS

MONITORING



Software for Vendor Risk Teams

A vendor record that knows what the vendor touches — data, systems, entities, regulations — is a vendor you can tier honestly. Scoring separates inherent exposure from control effectiveness, and every tier can explain itself.

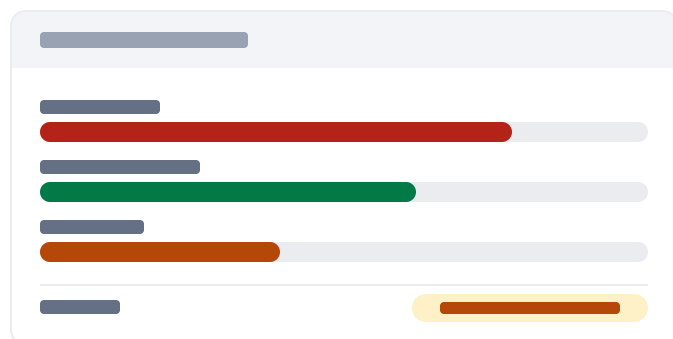
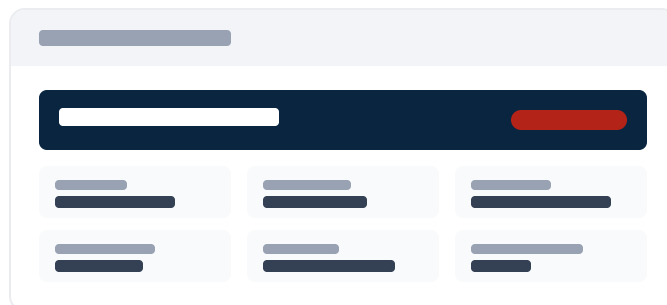
APPLICATIONS

[Third-Party Register](#)[Tiering & Scoring](#)[Assessments](#)[Due Diligence](#)[Issues](#)[Knockout Rules](#)

A register with context

Each third party carries its legal entity, jurisdiction, type, lifecycle stage, data classification, system access, criticality, regulatory scope and revenue dependency — and links to the enterprise risks it feeds.

- Lifecycle from prospect to offboarded
- Contacts, documents and history per vendor



Tiering you configure

Inherent factor rules set exposure; control domains and scoring bands set effectiveness; residual maps to a tier. Knockout rules stop a vendor regardless of score, and every tier records why.

- Weighted tier factors per scoring profile
- Overrides recorded with a reason

Assessments & due diligence

Questionnaires with scored responses go to the vendor at the depth the tier demands. Due-diligence requests are tracked to a decision; issues raised along the way become findings with owners.

- Issues linked to the question that raised them
- Enterprise scoring baseline across vendors



Software for Procurement & Contract Owners

A vendor is only as risky as what you engage them for. Engagements scope the services, data and systems involved; contracts carry obligations, renewals and approvals; the exit plan is a record with a status.

APPLICATIONS

Engagements

Contracts & Obligations

Renewals & Approvals

Contacts

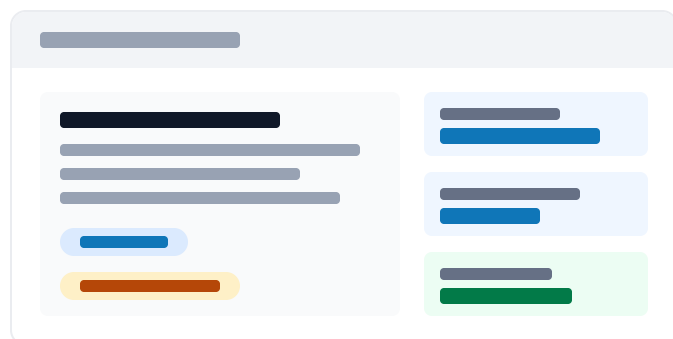
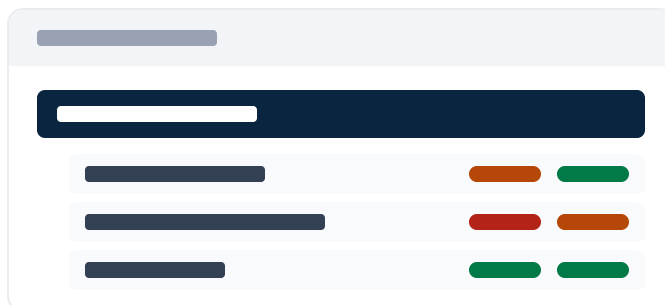
Services & Assets in Scope

Exit Plans

Engagements that scope the risk

Each engagement names the services, data and systems in scope, the entities it serves, and carries its own inherent and residual tier — so one vendor with three engagements is three risks, not one.

- Linked to the services and assets it touches
- Engagement types and status lifecycle



Contracts & obligations

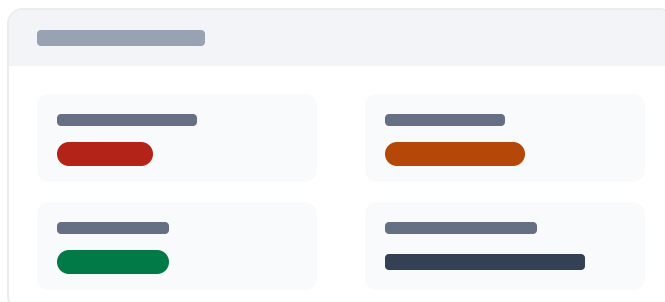
Contract type, governing law, value and currency, auto-renewal with its notice period, and the obligations the vendor owes you. Reviews route through approval and active contracts roll up to the vendor.

- Renewal notice before the contract auto-renews
- Confidential contracts with restricted access

Resilience & exit

Flag engagements that support a critical function, rate how substitutable the vendor is, and keep the exit plan's status and last test date on record. Produce the register of ICT arrangements at entity or group level.

- Substitutability and exit-plan status
- Register of ICT third-party arrangements



Software for Ongoing Monitoring

Onboarding is one day; the relationship is years. Reassessment, monitoring and evidence refresh run on the cadence you set per tier, fourth-party exposure is aggregated across vendors, and indicators trip before the annual review does.

APPLICATIONS

Review Cadence

Fourth Parties

Concentration

Key Risk Indicators

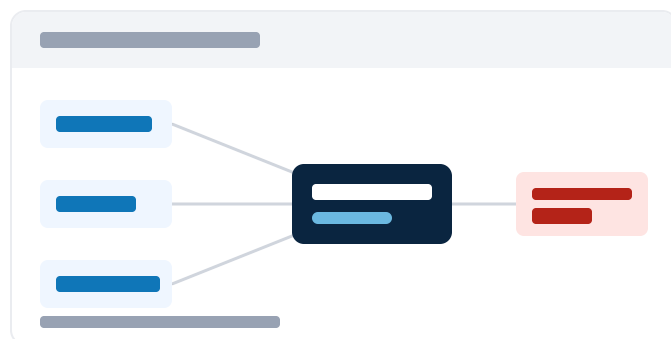
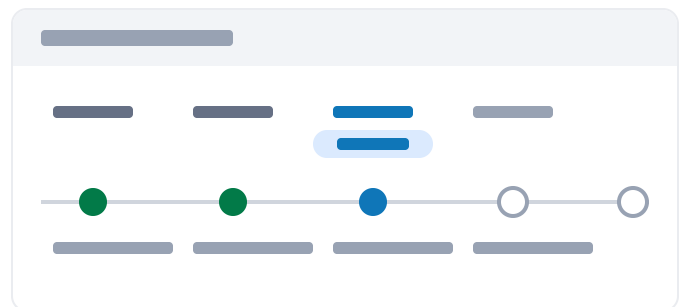
Escalation

Dashboards

A cadence you set

Review schedule rules decide, by tier and vendor type, how often a vendor is reassessed, monitored and asked for fresh evidence — and when an overdue review escalates. One rule can cover many vendors.

- Next assessment date on every vendor
- Overdue reviews escalated to owners



Fourth parties & concentration

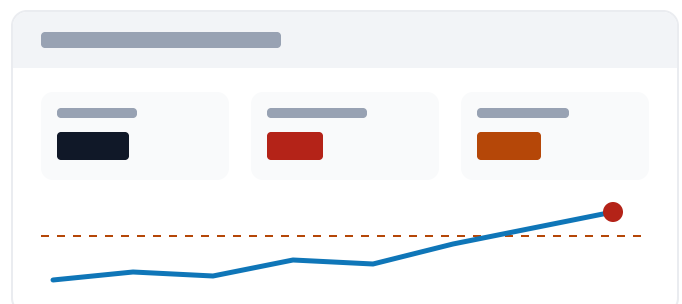
Record the suppliers behind your suppliers and the dependencies between vendors. Every link aggregates into an exposure per fourth party, so a shared hosting provider shows up as one risk, not twelve.

- Exposure summaries and concentration alerts
- Revenue dependency and concentration notes

Indicators, escalation & dashboards

Third-party indicators carry thresholds and a reading history; a breach is an escalation reason in its own right. The dashboard shows tiers, expiries, open issues, overdue reviews and concentration.

- Vendor lifecycle history end to end
- Third-party findings in the same queue



One platform underneath every vendor

Third parties, engagements, contracts, assessments and issues share one record set, one set of people and one workflow engine — beside enterprise risk, compliance and the asset register on the same platform.

WORKFLOW DESIGNER

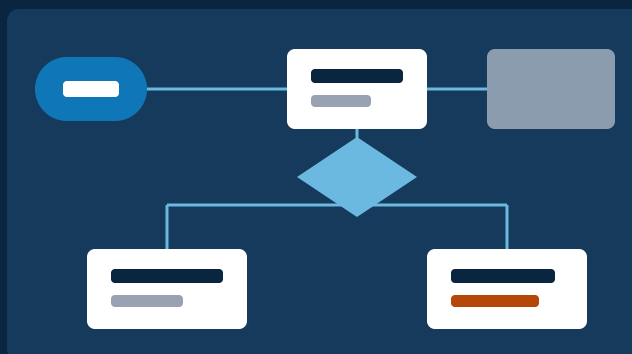
No code — but real logic.

Vendors, engagements, contracts and due-diligence requests each follow a lifecycle you can reshape: structured conditions, scheduled and date-field triggers, escalation ladders and role-gated approvals, 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 vendor's page shows its engagements, contracts, the assets and services it touches, its fourth parties and the risks it contributes to.



Dashboards and reports

A third-party dashboard with tiers, expiries, open issues and concentration; generated reports stored alongside the evidence 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.

VENDOR RISK

Third-Party Register
Tiering & Scoring
Questionnaires & Assessments
Due Diligence
Issues
Knockout Rules

MONITORING

Review Cadence
Fourth Parties
Concentration
Key Risk Indicators
Register of ICT Arrangements
Dashboards

ENGAGEMENTS & CONTRACTS

Engagements
Contracts & Obligations
Renewals & Approvals
Contacts
Services & Assets in Scope
Exit Plans

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 vendor register with tiers, contracts, assessments, issues and fourth-party exposure already in motion.

www.sentinelunity.com
support@sentinelunity.com