GENESECURE

GENELLIPSE

OPERATIONS & RESILIENCE

Vendor & Third-Party Risk

Supplier oversight continues beyond onboarding

Core capabilities

The main activities and the information they connect.

Vendor inventory and tiering

Record criticality, service scope and ownership.

Due diligence and assessments

Coordinate initial and periodic due diligence.

Contract terms and renewals

Connect terms and renewals to obligations.

Continuous risk monitoring

Review changes in supplier risk signals.

From daily work to oversight

Supporting functions keep decisions and evidence current.

Concentration and fourth-party mapping

Inspect shared providers and downstream dependencies.

Findings and remediation

Track agreed actions and completion evidence.

Vendor dependency graph

Relate suppliers to services and obligations.

Regulatory requirement mappings

Map the relevant requirements to oversight work.

How the work moves

A proposed operating workflow for your evaluation.

01

Onboard

Record ownership, criticality and due diligence.

02

Connect

Link contracts, services and dependencies.

03

Monitor

Review changing cyber and business risk signals.

04

Resolve

Track findings through the accountable vendor owner.

Supplier risk reaches the business service

The relationships that make the workflow understandable.

01

Vendor

The contracted provider and accountable owner.

02

Dependency

Subcontractors and shared service providers.

03

Service

The activity that could be disrupted.

04

Response

An approved remediation or continuity action.

Several vendors share one cloud dependency

An illustrative service review finds that apparently separate suppliers rely on the same underlying provider.

Team response

Confirm the dependencies, assess concentration across services, and coordinate the vendor and continuity owners on the response.

Decision point

Independent contracts do not necessarily mean independent operational risk.

What changes for your team

The practical value to evaluate against your current process.

A view beyond the onboarding file

Changing supplier signals stay connected to services, contracts and accountable owners.

Better visibility of concentration

Shared dependencies reveal exposure that separate vendor assessments can miss.

Where this module connects

Confirm the interfaces and available data for the intended deployment.

Sources	Vendor records, contracts, assessments and permitted monitoring feeds.
Connected modules	Cyber Risk Intelligence, Continuity and Enterprise GRC.
Working outputs	Owned findings, concentration views and assessment history.

What to validate in your evaluation

Use a representative case and agree the acceptance evidence before expansion.

Vendor owner	Approve assessments and manage remediation commitments.
Evidence	Keep assessment versions, contracts and dependency sources.
Measure	Track expired assessments, unresolved findings and concentration exposure.

A focused walkthrough Vendor & Third-Party Risk

Bring a representative workflow, its source records and the people who own the decision.

Starting point

Several vendors share one cloud dependency

Working session

Follow the case from input through review to retained evidence.

Genellipse.com

genesecure.ca