

START HERE

GeneSecure Platform overview

Connected risk. Governed decisions.
Evidence that stays with the work.

From separate signals to a shared risk record

The platform brings security and governance teams into the same operating context.

The starting problem

Findings, controls, supplier records and committee reports live in different tools.

The platform approach

Connect the source evidence to business risk, accountable owners and reviewable actions.

The common foundation

Each module uses the same underlying information and governance.

01

Data fabric

Connect source records in a shared risk graph.

02

Modules

Run the work for the relevant risk domain.

03

Cortex

Prepare cited answers and proposed actions.

04

Evidence ledger

Keep the decision and its supporting trace.

Risk and GRC

Four modules connect enterprise oversight to control and regulatory work.

Risk Management

Registers, indicators and owned treatments.

Compliance

Control mappings, tests and evidence.

Enterprise GRC

Shared governance across risk, resilience and privacy.

Regulatory Intelligence

Change monitoring and obligation ownership.

Financial risk and model oversight

Quantitative analysis connects to the governance of the models behind it.

Financial Risk

Liquidity, market and credit analysis with scenarios, limits and assumptions.

Model Risk & AI Governance

Model inventory, validation, performance monitoring and review conditions.

Security operations and cyber intelligence

Security signals support investigation and enterprise risk decisions.

Cyber Defense

Detection, exposure context and owned SOC cases.

Trust Center

Controlled publication and document access.

Cyber Risk Intelligence

Explainable ratings and material exposure priorities.

Questionnaire Automation

Cited draft answers and reviewer approval.

Operational resilience and suppliers

Services, recovery plans and external dependencies connect in the same risk view.

Business Continuity

Service mapping, impact analysis, recovery plans and exercises.

Vendor & Third-Party Risk

Due diligence, ongoing monitoring and dependency concentration.

Cortex supports the review process

AI assistance carries source context and operates within configured policy.

01

Ask

Use the permitted risk and control records.

02

Draft

Prepare a cited answer or proposed action.

03

Review

Apply policy and the required human approval.

04

Trace

Retain the run and decision evidence.

A supplier incident crosses several teams

Illustrative scenario: a critical supplier reports a security incident affecting an important business service.

Connected workflow

Security validates the exposure. Vendor owners assess the dependency. Continuity teams review recovery options.

Shared decision

The risk owner reviews the combined evidence and approves the treatment. Compliance retains the relevant control evidence.

Integrations start with the tools you use

The chosen deployment determines connector availability and the permitted scope.

Security context	Asset, endpoint, cloud, identity and vulnerability signals.
Business context	Services, suppliers, controls, obligations and model records.
Action and evidence	Case workflows, treatment owners and retained review records.

Different teams, connected responsibilities

A common record helps teams coordinate while keeping decisions accountable.

Risk and compliance

Own appetite, obligations, control conclusions and committee reporting.

Security and operations

Investigate findings, approve response and validate recovery.

Model and AI governance

Challenge models and define the permitted AI workflow.

A practical first evaluation

Select one workflow that reveals the relationships between teams.

01

Scope

Agree the business question and owner.

02

Connect

Use representative records and approved access.

03

Review

Test normal cases, exceptions and approvals.

04

Measure

Compare evidence quality and effort with the baseline.

What this collection represents

Based on GeneSecure's public product pages reviewed on 28 September 2026.

Documented scope

One overview and 13 named module presentations. The shared data foundation and evidence ledger appear throughout.

Evaluation context

The source is a product demonstration. Confirm configured capabilities and assurance status. Framework alignment does not mean certification.

Your risk workflow, connected

Start with the platform overview, then explore the module closest to your team's work.

Explore

Choose a module from the presentation collection.

[Genellipse.com](https://genellipse.com)

Discuss

Bring a real workflow and the evidence your decision needs.

genesecure.ca