Turn a risk into a decision someone owns.

Review possible failures through their business impact, likelihood, controls and remaining uncertainty.

Risk record

Field	What to document
Scenario	A concrete way the system could fail
Impact	The users, records or business process affected
Control	A prevention, detection or recovery measure
Owner	The person who accepts or resolves the remaining risk

Use scenarios rather than abstract labels

Data risk is too broad to guide implementation. A scenario such as an unauthorised user retrieving a customer document identifies a boundary that can be tested.

Review residual risk after the control

A control changes the risk rather than making it disappear automatically. Record what it does not cover and when the decision should be revisited.

Describe a risk as a concrete event

A useful risk statement identifies what could happen, why it is plausible and the consequence for the business. “AI risk” or “integration risk” is too broad to guide action. A more useful statement might describe an assistant retrieving a restricted document after a permission change, or a timed-out request creating a duplicate order when retried.

Record the affected workflow, the people or records exposed and the assumptions behind the assessment. Consider existing controls before proposing additional ones. Distinguish a known defect from an uncertain future event, and identify the person who owns the business consequence. A risk register becomes practical when it supports a decision rather than merely listing concerns.

Choose controls that address the cause

Compare ways to avoid, reduce or contain the event. For restricted retrieval, that may involve access checks, permission-change propagation and tests using representative roles. For uncertain writes, it may require idempotency and reconciliation rather than more aggressive retries. Explain what each proposed control changes and what remains possible after it is applied.

Match the effort to the consequence and the uncertainty involved. A small experiment may establish whether a suspected dependency is a genuine problem. A high-impact boundary may need stronger evidence before release. Record the cost and operational responsibility of a control as well as its expected benefit. A safeguard that nobody can maintain may not remain effective.

Review residual risk deliberately

After implementing a control, verify its behaviour with a representative failure case. Record the evidence and the limitation that remains. If the business accepts that limitation, identify the authorised decision-maker and the condition that will trigger another review.

Revisit risks when the workflow, data, user population or provider changes. A control designed for an internal pilot may be insufficient when the system gains write access or is opened to customers. Use incidents and near misses to improve the assessment. Risk management is a continuing conversation about concrete operating choices. This resource does not establish that a system meets a particular regulatory or contractual requirement.

Who should accept a material business risk?

An authorised business owner with enough context to understand the impact and alternatives. Engineering supplies evidence and explains technical limitations.

Read the current resource online

https://cobnex-review.rgcsekaraa.workers.dev/impact/