

Vendor risk assessment (sample)

Sanitized decision trail excerpt

Inherent risk

Medium (data sensitivity: medium; access: medium; criticality: medium).

Control strength

Meets baseline identity, logging, and incident response controls with evidence available under agreement.

Open items

SOC 2 report requested under agreement. Next review at renewal or upon material scope change.

Decision and conditions (sample)

Time-boxed follow-ups prevent drift

Decision

Approve with conditions.

Conditions

Provide updated SOC 2 report under agreement within 30 days. Provide updated subprocessor list on next quarterly review.

Proof expectations

Conditions are closed only when evidence artifacts are captured and indexed with dates.

Reviewer note (sample)

How to avoid scope drift

Keep scope explicit

Record what service is in scope, how it is used, and what data is exposed. If usage changes, re-score risk.

Avoid over-collection

Request only what you need based on tier (criticality + data exposure). Over-collection slows reviews and creates storage risk.

Retain a decision trail

Keep the decision memo/log and tie follow-ups to specific artifacts with dates. Auditors value traceability.