

COMPLIANCE & SECURITY · CHECKLIST

Vendor Risk Review Checklist

For operations and technical leaders who need a fast, consistent way to assess third-party tools before and after they're connected to company data.

How to use this: Tier each vendor by what it touches, then apply the matching level of review before signing up or renewing.

Vendor Tiering

Sort current and prospective vendors into tiers based on what they can access.

Vendor	What It Touches	Tier (Critical / Standard / Low)	Last Reviewed

Core Review Questions (Critical and Standard Tier Vendors)

- ☐ What specific data can this vendor access, and is that access scoped to only what's needed?
- ☐ Where is the data stored, and does that location matter for our customers' requirements?
- ☐ Does the vendor have a public security page, certification, or documented security posture?
- ☐ What is the vendor's process and commitment for notifying us of a security incident?
- ☐ Does the vendor's own subprocessor list introduce any additional risk we should know about?
- ☐ What happens to our data if we cancel? Is it deleted, exportable, or retained?

Operational Dependency Check

How critical is this vendor to a core workflow? What breaks if it goes down for a day?

How difficult would it be to replace this vendor if pricing, features, or terms changed unfavorably?

Has an alternative ever been evaluated, even informally?

Is there a single point of failure created by relying on this vendor exclusively?

Low-Tier Vendor Fast Check

- ☐ Vendor does not have access to customer data, source code, or payment information.
- ☐ Vendor is used by a limited number of people for a non-critical function.
- ☐ No further review needed beyond confirming these two conditions.

New Vendor Intake Habit

- ☐ New vendors are checked against this tiering before being connected to real data.
- ☐ Critical-tier vendors require sign-off from a named person before go-live.
- ☐ Vendor list and tiers are revisited at least twice a year.
- ☐ Any vendor with a known incident or acquisition is re-reviewed promptly.