ThirdNexa
Third-party risk management for financial services

Vendor Risk Assessment Checklist

A working checklist for RIAs, broker-dealers and funds: what to assess for every vendor, and the steps your firm runs to reach a documented decision. Your firm applies its own criteria and records every decision — no software or checklist labels a vendor approved.

A. Six factors to assess for every vendor

- [ ] **1. Access to customer information**
  Does the vendor access, store or process nonpublic personal or sensitive customer information? This drives Regulation S-P scope.
- [ ] **2. Critical business function**
  Would an outage disrupt trading, client service, custody, reporting or recordkeeping?
- [ ] **3. Systems and data access**
  What networks, applications and data sets can the vendor reach, and with what level of privilege?
- [ ] **4. Use of AI and subcontractors**
  Does the vendor rely on AI tools or fourth parties that handle your firm's data?
- [ ] **5. Security evidence**
  SOC reports, policies, penetration-test summaries and insurance — current, complete and reviewed.
- [ ] **6. Contract protections**
  Incident notice, safeguards, audit rights, data return and termination terms.

B. Six steps from inventory to documented decision

Step 1 — Build the inventory

- [ ] List every vendor with its services, owner and contacts
- [ ] Note the data and systems each vendor touches
- [ ] Record which person at the firm owns each relationship

Step 2 — Assign a risk tier

- [ ] Apply the firm's own criteria to rate the vendor
- [ ] Weight access to customer information heavily (Reg S-P)
- [ ] Let the tier set review depth and frequency

Step 3 — Run due diligence

- [ ] Send the questionnaire and collect evidence
- [ ] Review SOC reports, policies, test summaries and insurance
- [ ] Record dated review notes and findings

Educational information only, not legal advice.
thirdnexa.com · sales@thirdnexa.com · 847-877-0365

B. Six steps (continued)

Step 4 — Review the contract

- ☐ Check incident-notice, safeguards and audit-rights clauses
- ☐ Check data return and termination terms
- ☐ Record what is present, missing or in negotiation

Step 5 — Decide and document

- ☐ Your authorized reviewer records the outcome
- ☐ Record accepted risks and any remediation with owners and due dates
- ☐ Sign and date the decision record

Step 6 — Monitor and repeat

- ☐ Track expiring documents and insurance
- ☐ Record incidents and follow-up as they arise
- ☐ Set the next review date and keep the assessment current

Decision record — complete for each vendor

Vendor: _____

Risk tier (your criteria): _____

Outcome (your decision): _____

Authorized reviewer: _____

Date: _____

Evidence reviewed: _____

Accepted risks: _____

Next review date: _____

Notes: _____

Keep this checklist with each vendor's file. Your firm's criteria, decisions and evidence — not this document — are what an examiner reviews.

© ThirdNexa LLC. Last reviewed October 16, 2026. Vendor risk assessment checklist for financial-services firms.