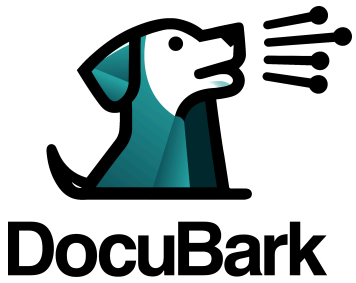


A New Model for Vendor Due Diligence

Designing Third-Party Reviews for the Modern Enterprise

by Jonathan Mandell
Founder, DocuBark
Third-Party Risk & Vendor Security Practitioner
v1.0
November 2025

Executive Summary

Third-party risk due diligence is broken. The traditional questionnaire-centric approach has become slow, inefficient, and inaccurate; it is costly to run and, perhaps most importantly, creates constant friction for the business it is meant to support.

This paper proposes a next-generation model for vendor due diligence: start from inherent risk and vendor size, rely on strong external signals and regulatory posture for large providers, and concentrate real, meaningful diligence on the small, high-impact vendors where risk is truly concentrated.

Questionnaires may still play a limited supporting role, but the center of gravity shifts toward a faster, more transparent, and more defensible method of assessing third parties.

1. The Current Model: **A Ritual, Not a Control**

In the standard model, vendors are pushed through some version of:

1. Intake
2. Scoping
3. Security questionnaire
4. Follow up questions
5. Risk sign off

The questionnaire step has become a ritual. It is performed because policy says so, because auditors expect to see documents, and because “this is how we have always done it”.

In practice:

- Large enterprise vendors reply with prepackaged answers that reveal little.
- Small vendors reply with improvised answers that are hard to trust.
- TPRM teams spend more time managing questionnaires than managing risk.

The result is governance theater: a lot of visible motion, but very little real progress in identifying and managing third-party risk or changing actual exposure.

2. Large Vendors: **The "We Have a Problem With Workday" Trap**

2.1 How questionnaires go wrong with large enterprise providers

When you send a 100 line spreadsheet to Workday, Twilio, Salesforce, or a similar large provider, several things happen.

- **You have almost no leverage.** They will not re-engineer their controls or rewrite their standard language to satisfy one customer's form.
- **You do not get bespoke insight.** You get standard security responses, SOC 2 mappings, and Trust Center links that are already public.
- **You do not get meaningful differentiation.** On paper, every large vendor has encryption, IAM, training, logging, and incident response.

The process feels busy, but it rarely changes your conclusion or outcome.

2.1.1 Small differences in answers, almost no difference in risk

Even when large vendors give slightly different answers, the practical impact is often minimal.

Examples:

- One vendor may require explicit customer approval before support can access production data. Another may allow support access by default within strict internal controls.
- One vendor may keep more of its contractor workforce in one geographic region. Another may distribute contractors across several countries that are all acceptable to you.
- One vendor may phrase retention settings one way and another slightly differently, even though both are operating within common regulatory and commercial expectations.

These differences can show up as different answers in a spreadsheet, but they do not usually change the overall risk profile of the vendor in a material way. Each company is making its own tradeoffs inside a broadly acceptable range.

Treating every small variance in an answer as a trigger for deep investigations or elaborate "compensating controls" is a misallocation of effort. The more realistic view is that:

- At the level of the specific business process, there are local differences in how vendors operate.
- At the level of overall vendor risk, these small differences rarely justify major delays or escalations.

Questionnaires tend to overemphasize these micro differences and underemphasize the bigger picture.

2.2 The recurring “problem with Workday” moment

Every TPRM team eventually hits the same scenario, often multiple times per year:

1. A large, established vendor is going through review.
2. The questionnaire or contractual negotiation gets stuck on a detail.
   A wording in your form does not match their policy, they will not sign your custom appendix, or they simply refuse a specific checkbox.
3. The issue escalates internally, and suddenly TPRM is in a meeting saying:
   “We have a problem with Workday.”

Everyone in the room feels the disconnect.

- The business knows Workday already runs payroll and HR for thousands of large enterprises.
- They know your company is not realistically going to replace Workday or block a key project.
- They intuit that the holdup is procedural, not about a concrete, unmanageable risk.

At that moment, the business sees the delay as process friction that adds little value. The TPRM team is left defending a position that even they do not fully believe. The issue is not that Workday is unsafe. The issue is that Workday did not participate in an internal questionnaire ritual in exactly the way the process expected.

This dynamic:

- Erodes trust in TPRM as a partner to the business and encourages workarounds and exceptions.
- Shifts conversations from “what is our real exposure” to “how do we get around our own process”.

3. Large Vendors: **Size, Incentives, and Real Risk Signals**

3.1 Size and public metrics tell you more than a spreadsheet

The core question for any vendor is simple: **How much damage could they realistically do to us if something goes wrong?**

For large providers, some of the strongest indicators of their security posture are public facts:

- Customer base and market role, for example, core payroll, identity, cloud infrastructure, messaging.
- Regulatory footprint and certifications, for example, SOC reports, ISO, PCI, FedRAMP, financial, utilities or healthcare regulation (NYDFS, NERC, Hipaa).
- Operational and incident history, for example, public breaches, outage history, transparency reports.

These signals are not perfect, but they are often more predictive than self scored checkbox answers.

3.2 Incentives as a security control

A large vendor that suffers a major breach is not just embarrassed. They are at real risk of:

- Losing billions in enterprise value.
- Losing critical customers and contracts.
  Attracting regulatory scrutiny and litigation for years.
- Permanently damaging their brand.

SolarWinds is a clear example. One incident reshaped the company's reputation and the way the market views the brand. Incidents at that scale become existential.

Large enterprise vendors live under that threat constantly. Their board, investors, largest customers, and regulators all push them toward better security, regardless of your questionnaire.

3.3 What about the argument that big companies can be careless

It is true that large companies can still be careless and irresponsible. There have been major breaches at global brands with large security budgets.

Root causes in those cases are usually things like:

- Legacy and complexity.
- Cultural tradeoffs that favor speed or revenue over hardening.
- Fragmented ownership and slow governance.
- A single employee mistake or chance event that slips through, combined with a failure of layered defenses.

None of this shows up clearly in a custom spreadsheet. It shows up in:

- Real incident history.
- The quality and speed of public incident response.
  Regulatory action.
- Patterns across multiple customers and industries.

If a large vendor worries you, the right response is to:

- Treat them as an infrastructure or systemic risk.
- Model your dependency and blast radius.
- Implement compensating controls on your side, for example logging, segmentation, backups, layered providers, and exit plans.

Sending a bigger questionnaire does not move those structural forces.

4. Small Vendors: **Inherent Risk, Controls, and Viability**

Questionnaires are at their weakest with small vendors, especially startups and niche software providers.

Here the right anchor is inherent risk. What are we asking this vendor to do for us, and what happens if they fail or leak data?

4.1 Low inherent risk small vendors

Examples:

- A narrow tool with no access to production data.
- An internal productivity tool with limited exposure.
- A niche reporting or collaboration add-on that only touches non sensitive content.

If the inherent risk is low:

- The blast radius is limited by design.
- The main questions are:
    - Can we shut them off quickly if needed?
    - Are we exposing any data that would meaningfully hurt us?

In this context, the exact state of their SIEM, password policies, or incident runbook matters much less than:

- Data minimization.
- Access restrictions.
- Contractual and technical off ramps.

A heavy questionnaire is misaligned. You are spending more time interrogating a vendor than it would cost to contain the impact if they failed.

4.2 High inherent risk small vendors

The more precarious case is a small vendor with high inherent risk:

- A startup that processes core customer or transaction data.
- A boutique firm deeply embedded in a critical workflow.
- An AI provider that ingests large volumes of sensitive input.

Here, traditional due diligence can actually make sense, but not in the form of a standalone spreadsheet. For these vendors, meaningful review should include:

- Real evidence:
    - SOC 2 or equivalent if it exists.
    - Architecture and data flow diagrams.
    - Configuration screenshots.
    - Pen test results and remediation status.

- Direct conversations with leadership:
    - How the founders and technical leaders think about security and reliability.
    - How they prioritize security given limited resources.

- Jointly designed compensating controls:
    - Data minimization.
    - Environment isolation.
    - Logging and monitoring arrangements.
    - Incident and notification expectations.

A questionnaire can support this process, but it should not be the centerpiece. The real insight comes from understanding how the company operates, not from collecting generic yes or no answers.

4.3 Financial health and ongoing viability

For small vendors, security posture is only one dimension of risk. Financial health and ongoing viability matter too.

- For low inherent risk small vendors, financial fragility mostly translates into inconvenience: a vendor shutting down might disrupt a minor workflow, but you can replace them or do without. Light checks and short, flexible contracts are usually enough.
- For high inherent risk small vendors, you need a bit more assurance that they can sustain the controls you care about. That can mean looking at:

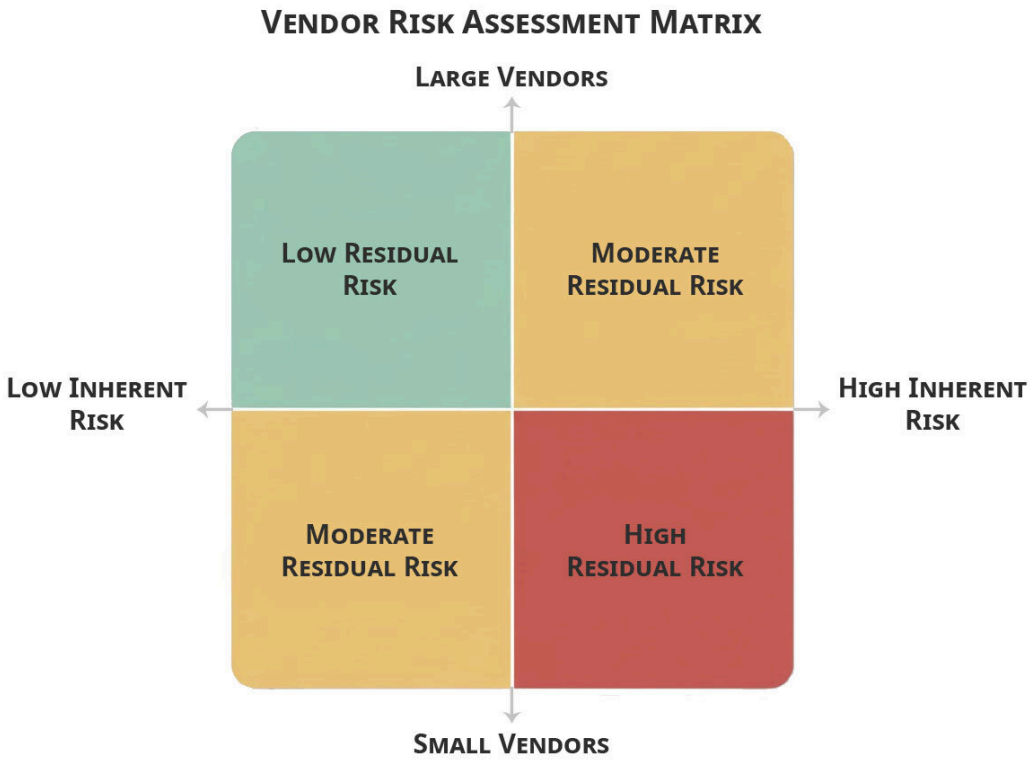
    - Funding and cash runway.
    - Revenue concentration and customer churn.
    - Growth plans relative to security resourcing.
    - Basic financial information where it is reasonable to request it.

You do not need a full audit, but you do need enough context to decide if you are comfortable depending on them. Contracts with clear exit and data export rights, avoiding single points of failure, and scheduled check-ins on both security and viability are often more valuable than another spreadsheet.

5. Mapping the Landscape: **Inherent Risk vs Vendor Size**

A simple way to visualize this is as a Cartesian plane.

- Horizontal axis: Inherent risk of the engagement
  Low on the left, high on the right.
- Vertical axis: Size of the vendor
  Small at the bottom, large at the top.



This gives four quadrants.

1. **Top left**
   Large vendor, low inherent risk.
   Example: a widely used platform providing a non critical internal utility.
   - Risk is modest.
   - Focus on basic segmentation and straightforward contracts.

- Questionnaires are unlikely to change the decision.

2. **Top right**
   Large vendor, high inherent risk.
   Example: cloud infrastructure, core HR, core payments.

   - This is a systemic dependency, but the vendor is already heavily scrutinized by the market.
   - Use public evidence, certifications, contracts, and compensating controls on your side.
   - Questionnaires mostly create internal friction without meaningful risk change.

3. **Bottom left**
   Small vendor, low inherent risk.
   Example: niche productivity tool with no sensitive data.

   - Design the relationship so the blast radius is tiny.
   - Make it easy to turn off, and keep important data out of scope.
   - Minimal due diligence is appropriate.

4. **Bottom right**
   Small vendor, high inherent risk.
   Example: young company processing core customer data or sitting in a critical workflow.

   - This is where your real vendor risk lives.
   - This quadrant demands deeper work on security, architecture, and financial viability.
   - This is where you decide how much risk you are willing to take on for the benefits of innovation or speed.

Three of these quadrants do not justify a heavy questionnaire as the main tool. The bottom right quadrant, small and high inherent risk, is where you actually need serious attention and a conscious choice about risk appetite.

Every company has to make its own determination about how much exposure it is willing to accept in that quadrant, and what compensating controls or contract structures are required.

6. Compliance: **Are Questionnaires Required**

Most regulatory regimes and frameworks require that you:

- Assess third party risk.
- Understand how vendors protect your data and services.
- Monitor that risk on an ongoing basis.

They typically do not require a specific tool such as a security questionnaire.

Where organizations get into trouble is when:

- Internal policy hard codes questionnaires as mandatory for every vendor, and the policy is not followed.
- There is no documented evidence of any due diligence, whether questionnaires or other artifacts.
- Exceptions are granted informally without recorded risk rationale.

The problem in a best case scenario is a program not fit for purpose, and a worst case scenario of inconsistent & undocumented processes.

7. A Forward Looking Model: **Structured Signals Instead of Spreadsheets**

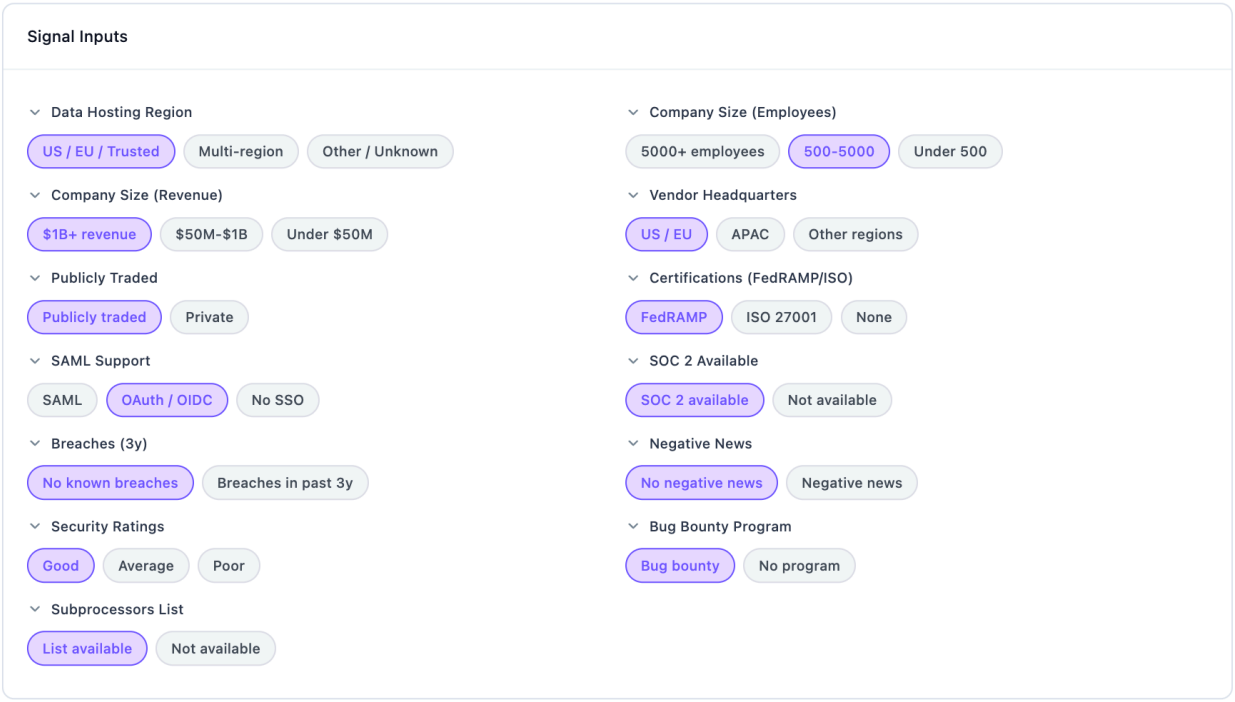
Instead of defaulting to questionnaires, a forward looking program can standardize on a small set of objective data points that describe a vendor's context and likely security maturity.

The idea is to capture who the vendor is and how they operate, without asking them to restate every control in free text.

Examples of useful structured signals:

- **Data hosting and geography**
    - Where is customer data hosted, for example US or EU or trusted regions versus other or unknown.
    - Whether the vendor operates in multiple regions or a single jurisdiction.
- **Company size and stage**
    - Rough employee and revenue bands, for example under 500, 500 to 5000, 5000 plus.
    - Public versus private, which hints at regulatory and disclosure expectations, including SEC reporting and cyber disclosure obligations for US public companies.
- **Independent assurance and capabilities**
    - Presence of SOC 2 or ISO 27001.
    - FedRAMP authorization for government facing services where relevant.
    - Support for SSO, such as SAML or OAuth / OIDC, for enterprise access control.
    - Existence of a bug bounty or formal vulnerability disclosure program.
- **Contractual Protections**
    - Security and privacy terms in the MSA, DSA, or DPA, including breach notification, subprocessor transparency, data residency, and limits on data use.
    - These terms act as enforceable commitments that can reduce residual risk when technical visibility is limited.
- **History and public signals**
    - Known breaches or significant negative news in the last few years.
    - External security ratings where available.

- Whether their subprocessors include clearly higher risk vendors and whether that is transparent.



These signals are not perfect, but they are:

- Easier to standardize across all vendors.
- More resistant to creative answering than long, free form questionnaires.
- Directly mappable into a simple residual risk view and into the “inherent risk versus size” picture described earlier.

A forward thinking policy can explicitly call out this kind of structured data collection as the primary evidence set for most vendors. Questionnaires, if used at all, are reserved for:

- High inherent risk vendors where independent evidence is missing.
- Specific gaps that cannot be answered through public and contractual documentation.

In other words, structured signals become the default control. Questionnaires become a narrow exception, not the center of the program.

8. Turning Signals Into Decisions: **Operating the Vendor Risk Program**

A modern vendor risk approach can be summarized in four principles.

8.1 Start with inherent risk and criticality

- What data is involved.
- What business process(es) depends on this vendor.
- What is the blast radius if they fail or leak data.

Let this drive the depth of review.

8.2 Prefer strong external signals over self attestation

For medium and large vendors, prioritize:

- Independent assurance, such as SOC 2, ISO, PCI, FedRAMP.
- Regulatory posture and existing oversight, including SEC compliance where applicable.
- Public Trust Center content, incident history, and contracts.
- Structured context signals like hosting region, size, certifications, and security ratings.

Use questionnaires only to close specific gaps that cannot be answered any other way, if at all.

8.3 Reserve heavy review for high impact small vendors

For the small set of vendors that land in the “small and high inherent risk” quadrant:

- Blend security, architecture, operations, and financial viability.
- Use meetings, evidence, and co-designed controls, not just forms.
- Make sure the relationship is structured so both sides can realistically uphold their commitments.

8.4 Document clear, simple decisions

For every vendor, large or small, record:

- The inherent risk.
- The evidence you relied on, including structured signals.
- Any significant concerns and how they are mitigated.

- The final decision: accept, accept with conditions, or reject.

This becomes your defensible story, both internally and with auditors.

8.5 Use MSAs, DSAs, and DPAs to shape residual risk

Contract language is one of the most direct levers you have to reduce residual risk for higher impact vendors. The MSA, DSA, and DPA should be treated as active controls, not just boilerplate.

For vendors that matter, contracts can:

- Limit data use and sharing to clearly defined purposes
- Set concrete breach and incident obligations
- Define expectations for subprocessors, especially higher risk ones
- Codify minimum safeguards that must be maintained

In many cases, vendors already have perfectly usable DSAs and DPAs. The goal is not to force “our paper” every time, but to confirm that their standard terms meet your risk requirements and only push for changes where there is a real gap.

8.6 Hand off to internal controls for how vendors are used

For many large vendors, the real risk is less “are they secure?” and more “how are we using them?” That includes:

- Big SaaS platforms where you control SSO, roles, logging, data export, and backups.
- Consulting and service firms where you decide which systems they can access and what data they see.

A modern model should:

- **Hand off clearly to internal control owners** (app owners, security, IT, data owners) once a vendor is approved, with specific responsibilities for access, configuration, and data handling.
- **Treat access and configuration as first class controls**: who gets into which systems, with what permissions, for how long, and how their activity is monitored.

For these vendors, due diligence is only the starting point. Your internal controls over access and configuration are what actually determine day-to-day risk.

Conclusion

Vendor questionnaires have become the default tool of third party risk management, but they no longer fit how risk actually works.

- For large enterprise vendors, questionnaires mostly generate internal conflict and delays. They do not change incentives, architecture, or real-world behavior.
- For small vendors, especially low inherent risk tools, questionnaires are disproportionate to the actual exposure. For high inherent risk startups, they are shallow compared to what you really need to understand.
- For both, better signals already exist in inherent risk, public evidence, incentives, financial health, and structured context data.

Used as a default, questionnaires do not just waste time. They create false comfort, push TPRM into unnecessary standoffs with the business, and distract attention away from the one quadrant where risk is truly concentrated: small vendors with high inherent risk.

The path forward is not to slightly streamline the spreadsheet. It is to replace it as the center of the program:

- Anchor everything in inherent risk and vendor size.
- Treat large vendors as systemic dependencies governed by market, regulatory, and economic pressure, not by your custom form.
- Focus real diligence on small, high impact vendors, combining security, architecture, and financial viability.
- Standardize on structured signals and independent assurance as primary evidence, with questionnaires as a rare exception.

A TPRM function that makes this shift will be faster, more accurate, and more credible. It will also be more cost effective and less resource intensive by concentrating effort where it actually changes outcomes. Most importantly, it will move at the speed of the business and focus attention on the vendors that matter most, instead of on managing questionnaires for everyone else.