How to tier your suppliers by risk

Third-party risk management (TPRM) is no longer a box-ticking exercise, it's a core part of protecting business resilience. As organisations rely more heavily on suppliers, partners, and service providers, the risks they carry can quickly become your risks too. A clear approach to TPRM helps you understand where you're most exposed, focus attention on the suppliers that matter most, and prove to customers, regulators, and investors that you take resilience seriously.

One of the most common recommendations is to "tier" your suppliers - placing them into high, medium, or low-risk categories. In theory, it sounds straightforward. In practice, many organisations struggle to do it consistently and meaningfully.

This guide gives you a structured, repeatable, and scalable approach to supplier tiering - from the questions you need to ask, to how to weight them, to how to turn scores into risk tiers.

Contents

Step 1 – Start with the right questions

To tier suppliers effectively, you need to probe the areas that reveal how much risk they introduce into your business. The core questions fall into five categories:

Data risk

- What data can they access in your own environment?
- What data do you pass them to protect in their environment?

Access & system risk

- What access to resources (systems, networks, privileged accounts) do they have?

Operational dependency

- Are you reliant on them for business-critical operations?
- How easy is it to replace them (availability of alternates, time, cost, disruption)?
- Would performance issues with their services directly impact your customers?

Regulatory & compliance

- Would a breach in their environment trigger regulatory obligations?

Reputation & strategic importance

- Is your reputation linked with theirs?
- Do they represent strategic importance or growth potential?

Step 2 – Understand the impacts

Each question ties back to a business impact. For a comprehensive model, consider:

Step 3 – Apply weightings and scoring

Not all questions carry equal importance. Weighting ensures critical risks have more influence on the final tier.

Here's an example of a framework you can adapt to suit your business:

Category	Question	Impact	Weighting	Y/N	Weighted Score
Data Risk	Can they access data in your environment?	Loss of IP/Asset, Financial, Reputation	20%	☐	Y = 0.20
	Do you pass data to them to protect in their environment?	Loss of IP/Asset, Service Disruption, Loss of Trust/Customer, Regulatory Scrutiny	15%	☐	Y = 0.15
Access & System Risk	Can they access resources such as systems, networks, and privileged accounts?	Service Disruption, Loss of IP/Asset, Systemic Impacts	15%	☐	Y = 0.15
Operational Dependency	Are you reliant on them for business-critical operations?	Service Disruption, Financial, Systemic Impacts	15%	☐	Y = 0.15
	Would it be difficult to replace them (time, cost, disruption)?	Cost of Replacement, Financial, Loss of Competitive Advantage	5%	☐	Y = 0.05
	Would performance issues with their services directly impact your customers?	Loss of Trust/Customers, Reputation, Financial	5%	☐	Y = 0.05
Regulatory & Compliance	Would a breach in their environment trigger regulatory obligations?	Regulatory Scrutiny, Financial, Reputation	15%	☐	Y = 0.15
Reputation & Strategic	Is your reputation linked with theirs?	Reputation, Loss of Trust/Customers	5%	☐	Y = 0.05
	Do they represent strategic importance or growth potential?	Loss of Competitive Advantage, Systemic Impacts	5%	☐	Y = 0.05

Once you have your weighted score, multiply by five in order to map your score to the tiers below.

Step 4 – Map scores to tiers

Once you've scored each supplier, you will need to place them into a risk tier – again, adapt to suit your needs:

Tier	Question	What It Means
1 - Critical	4.2–5.0	Supplier touches your most sensitive data/core systems or is difficult to replace. Requires continuous monitoring and may warrant in-house/hybrid control.
2- High	3.2–4.1	Supplier poses material risk to data, operations, or compliance. Requires thorough due diligence and regular reviews.
3 - Medium	2.0–3.1	Supplier has some importance, but failures are manageable. Standard onboarding checks and periodic review.
4 - Low	0–1.9	Supplier has minimal exposure. Basic assurance only.

However, tiering is only useful if it guides action. This should look something like the below:

- **Critical** – Full security questionnaire, evidence review, continuous monitoring, executive oversight.
- **High** – Security questionnaire + evidence, periodic review (12–18 months), contractual obligations for incident reporting.
- **Medium** – Standard onboarding checks, periodic review.
- **Low** – Minimal onboarding due diligence only.

Risks surfaced across all supplier tiers, through the TPRM process, should be incorporated into the Enterprise Risk Management framework and considered alongside the organisation's inherent risks for mitigation.

Step 5 – Recognise when outsourcing isn't viable

Some organisations face unmitigated supplier risks that are not only highly likely but could also prove existential in impact. When this happens, you need to ask yourself whether this function is too important to outsource at all.

In these cases, you have several options to consider:

- Retaining the function in-house.
- Splitting responsibility between internal teams and the supplier (hybrid model).
- Outsourcing to a more competent supplier who can demonstrate that they've managed the risk, within your risk tolerance.
- Applying additional compensating controls such as real-time monitoring or redundancy.

Step 6 – Keep it dynamic

One of the hardest parts of TPRM is that it is constantly changing. Supplier risk isn't static, which means you will need to reassess them when:

- You expand how you use the supplier.
- The supplier is acquired or changes ownership.
- They suffer an incident or regulatory breach.

Annual reviews or reassessments on contract renewal help ensure tiers stay accurate. Ensure that you retain audit rights and contract in TPRM assessment compliance when negotiating agreements with your suppliers.

Step 7 – Consider using a TPRM service if you have 20+ suppliers

Many organisations find that once they have 20 or more suppliers, it becomes more difficult to keep up with supplier assessments, assign and manage risk ownership appropriately across the business, and to satisfy requirements from CAF, DORA and ISO. At this point, it makes sense to consider partnering with a specialist TPRM service provider that offers:

Technology

- Continuous monitoring (security ratings, breach alerts, regulatory watchlists).
- Automated assessments and evidence requests.
- Central dashboards to track supplier risk across the lifecycle.

People

- Risk analysts who can interpret results and distinguish between noise and true risk.
- Collaboration with supplier managers who can escalate findings and maintain accountability.
- Security experts who can design proportionate controls and remediation actions.

Process

- Clear playbooks for onboarding, assessment, remediation and escalation.
- Defined thresholds for when to accept, mitigate, or reject supplier risk.
- Regular reviews tied to contract cycles and material changes.

A good TPRM service isn't just a questionnaire platform - it's a managed process that makes sure supplier risks are identified, prioritised, and acted upon, not just logged in a spreadsheet.

How to get started

1. Start with the list of suppliers that you've paid in the last 12 months. Assign business owners to each of the suppliers – these owners may own the budget/cost centre that pays the supplier, be signatories on the contracts or users of the provided service. If you're struggling to find a business owner, assign someone temporarily who understands or has a relationship with the supplier.

2. Ask the business owners to answer the questions featured in Step 3 of the framework for each owned supplier. In the absence of a business owner, the supplier might be asked for answers themselves. A spreadsheet template pre-populated with the framework questions can be found **here**.

3. Embed the Step 3 framework questions into the supplier onboarding and contract renewal processes.

4. The list of tiered suppliers can then be handed over to an outsourced TPRM provider, who will trigger the assessments, perform the reviews and proactively surface the risks from there.

Why getting TPRM right matters

When supplier tiering and third-party risk management are done well, the benefits reach far beyond compliance. Strong TPRM reduces the likelihood of a breach by identifying weak links before attackers exploit them. It strengthens regulatory resilience in the face of growing demands from FCA, PRA, GDPR, and DORA. It keeps the organisation running by minimising the chances of disruption from supplier failures, and it protects the bottom line by lowering the risk of costly incidents, penalties, or emergency replacements.

Perhaps most importantly, effective TPRM helps build trust. Customers, regulators, and partners can see that you take the security of your ecosystem as seriously as your own. In markets where security and resilience are now competitive differentiators, getting supplier risk management right is no longer a nice-to-have, it is a source of strength.

For an overview of TPRM and why it's importance is growing, read our recent **blog post**.

Ready to talk?

If you're ready to strengthen resilience, reduce supplier risk, and build greater confidence with stakeholders, our team can help. **Book your meeting** today.

Cybersecurity services to protect your organisation and respond to the threats of today and tomorrow.

Get in Touch
info@taloscs.com
www.talanoscs.com

UK
14 Upper Church Street,
Bellarmine House,
Chepstow,
NP16 5EX

South Africa
377 Rivonia Boulevard,
Rivonia,
Johannesburg,
2128

India
68, The GranCarmen
Carmelaram, Bangalore,
Karnataka,
560035