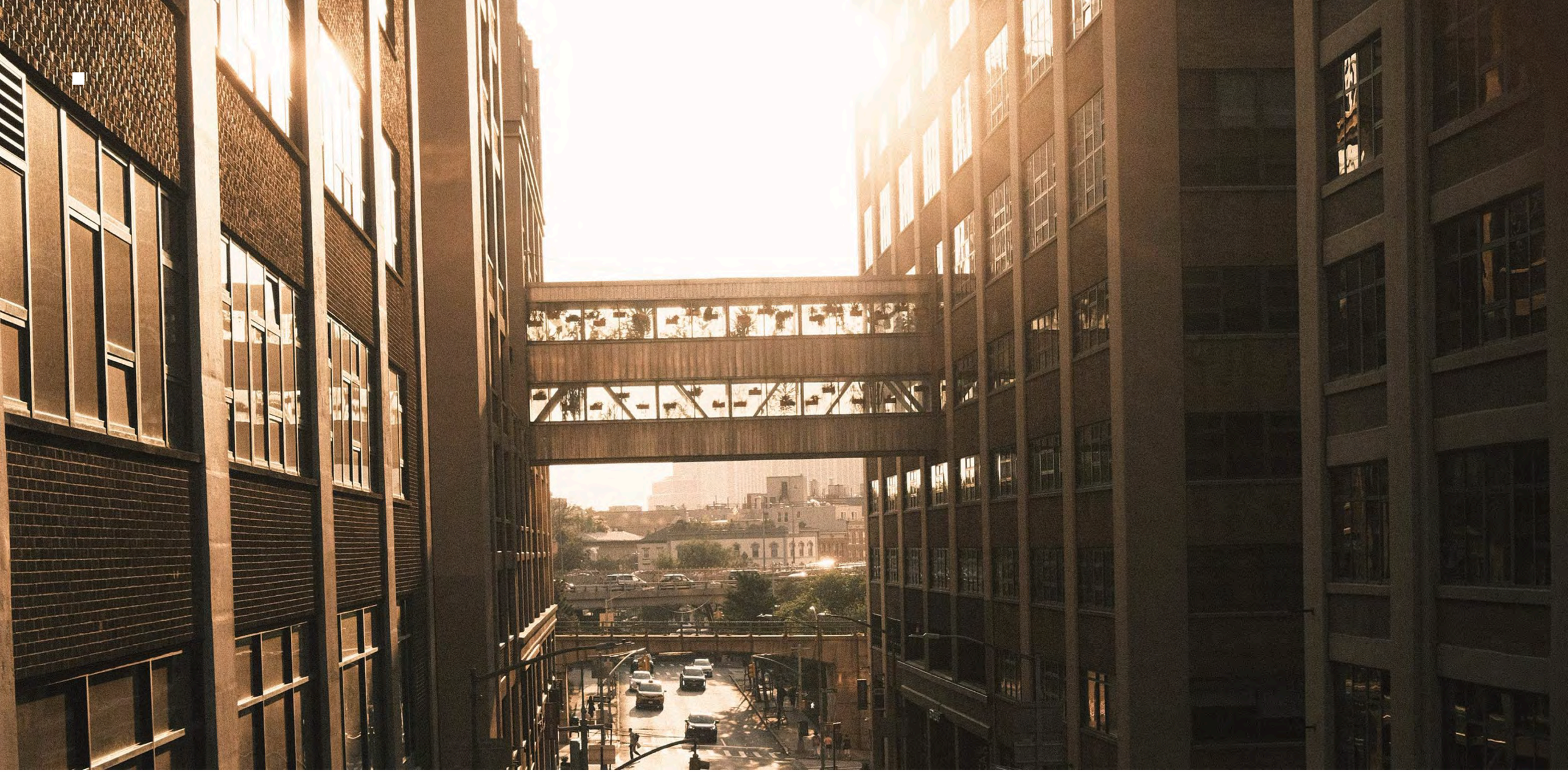
Vendor Risk Powered by UpGuard

Best-Practices Guide: Tiering and Classifying Vendors by Inherent Risk

A leader's guide to defensible vendor visibility.

This guide provides general best practices for vendor risk tiering.

It should be tailored to your organization’s industry, regulatory obligations, and risk appetite. Always ensure your approach meets any specific legal or compliance requirements relevant to your business.



Introduction

There's a fine line between managing risk and simply managing noise. If every vendor is a priority, none of them actually are. When you treat every vendor with the same intensity, you lose the ability to see the real threats. With a portfolio of hundreds or even thousands of unprioritized vendors, teams can struggle with time and resource allocation.

To maintain a defensible posture, you need a strategic way to focus: an inherent risk-based tiering system. By categorizing vendors by criticality and potential impact, you can scale your oversight where it matters most and reclaim your time.

For many teams, the challenge is not recognizing that vendor risk varies, but knowing where to start. Creating a consistent way to tier vendors is the first step to building a more focused and effective Third-Party Cyber Risk (TPCRM) program.

This eBook explains why and how to implement vendor tiering. It outlines clear criteria for classifying vendors and provides step-by-step guidance for applying them to your organization. The following best practices help you replace unclear thresholds and subjective judgment with a structured, repeatable approach to tiering vendors and assessing risk.

5 reasons to tier your vendors

How can you manage risk if you can’t measure it? In TPCRM, that starts with having clear answers to a few fundamental questions. Which vendors would materially disrupt the business if they failed or were compromised? Which relationships require continuous oversight, and which can be managed with proportionate effort?

And where should time and resources be focused to reduce real risk, not just generate activity?

Vendor tiering turns these questions from judgment calls into defensible decisions. The five reasons below explain why tiering is foundational to building a focused, scalable TPCRM.

1. Focused risk management

Grouping vendors by risk level enables your team to concentrate its oversight on the highest-risk vendors. This reduces poor risk management, burnout, and compliance gaps by avoiding spreading your efforts too thin.

2. Resource efficiency

Tiering eliminates unnecessary work. Instead of you having to subject all 800 vendors to the same due diligence continuously, you can scale the workload appropriately. You can justify appropriate control requirements for critical vendors while scaling back proportionate assessment depth to lower-risk vendors.

3. Improved business continuity

By prioritizing your focus on critical vendors, you can improve your organization's resilience by reducing risk where it would have the greatest impact. While a failure in a Tier 1 vendor could lead to a massive data breach or outage, a Tier 5 vendor would have a negligible impact. Tiering enables proportionate, risk-based expectations. It provides the time and prioritization needed to determine the appropriate level of control requirements and assessment depth based on actual vendor risk.

4. Compliance assurance

Tiering enables a defensible, risk-based approach to third-party oversight, helping organizations demonstrate alignment with regulatory and legislative expectations. Frameworks such as NIST CSF and ISO 27001 reinforce the need to prioritize controls and assessment effort based on risk rather than applying uniform treatment across all vendors.

5. Business and brand protection

Vendor tiering strengthens an organization’s TPCRM's defensibility. You can demonstrate to auditors, customers, investors, and other stakeholders that you have a rational method for managing vendor risks, which showcases maturity and good governance.

Logic of defensibility: Criteria for vendor risk tiering

Once you understand *why* vendor tiering matters, the next challenge is deciding *how* to evaluate vendors consistently and defensibly. Tiering decisions should not be based solely on instinct or individual judgment. They need clear inputs that can be applied uniformly across all vendors.

Risk criteria defines what you assess to understand a vendor's cybersecurity exposure and potential impact on your organization. These criteria break risk down into specific, observable factors such as system access, operational dependency, and recovery sensitivity. Rather than assigning a tier directly, each criterion contributes structured inputs that can be evaluated, compared, and scored consistently across vendors.

The criteria outlined below provide a practical foundation for this approach. By assessing vendors across defined categories, teams can apply context to third-party cyber risk and avoid one-size-fits-all decisions. These inputs then feed into a scoring framework, enabling vendors to be objectively grouped into tiers based on aggregated risk rather than subjective labels

Note on Tier Threshold Indicators

These indicators define the characteristic "threshold" for each risk level. We explore the qualitative profile of each tier (Critical to Transactional) in the **Defining Vendor Tiers** section.

Note on Scoring Logic

This logic determines how category inputs are weighted and calculated. A full breakdown of how these numbers map to final management strategies is explored in **The Quantitative Bridge**.

Risk Category	Assessment Criteria	Tier Threshold Indicators	Scoring Logic
Operational Continuity	Dependence on the vendor for day-to-day survival and revenue.	**Tier 1** Indispensable; the business stops immediately without it.	**Scaled (1-5):** Based on Recovery Time Objective (RTO) and availability of alternatives.
		Tier 2 Essential, but manual workarounds are in place for short periods.	
		Tier 3 Important but not mission-critical; failure is inconvenient but manageable.	
		Tier 4 & 5 Non-essential; nice-to-have or easily substituted.	
Data & System Access	The volume, sensitivity, and accessibility of organizational data.	**Tier 1** Access to core production databases or to millions of sensitive records.	**Scaled (1-5):** Based on the sensitivity of data handled and the level of system or production access granted.
		Tier 2 Access to sensitive data, but only in limited subsets or encrypted segments.	
		Tier 3 Read-only or limited access to non-critical systems.	
		Tier 4 & 5 No sensitive data access; handles only public info or contact details.	
Regulatory & Compliance	The vendor’s role in meeting legal or industry-mandated obligations.	**Tier 1** Supports "Critical Activities" as defined by regulators or legislative requirements.	**Scaled (1-5):** Based on the vendor’s role in meeting legal and contractual obligations, as well as their impact on regulatory standing if the vendor fails.
		Tier 2 Significant role in compliance but not a "critical" designation.	
		Tier 3 Standard vendor oversight applies (e.g., standard data clauses).	
		Tier 4 & 5 No meaningful effect on the organization's compliance posture.	

Risk Category	Assessment Criteria	Tier Threshold Indicators	Scoring Logic
Strategic & Supply Chain	The complexity of the vendor's own ecosystem and geography.	**Tier 1** Sole-source provider; significant long-term commitment.	**Scaled (1-4):** Based on geographical risk and concentration risk.
		Tier 2 Key strategic partner, but alternative vendors exist in the market.	
		Tier 3 Standard industry provider; replaceable with moderate effort.	
		Tier 4 & 5 Commodity provider; fully standardized and interchangeably replaceable.	
Security & Resilience (Optional)	The evaluation of existing controls, audit evidence, incident history, and AI governance.	**Tier 1** No baseline controls (e.g., Multi-Factor Authentication) and major recent breaches, or unregulated use of AI with sensitive organizational data.	**Residual adjustment:** Scaled (1-5) based on external assurance, incident history, and AI risk maturity. High-risk in this category can "bump" a vendor to a higher tier regardless of its inherent scores.
		Tier 2 Outdated audits (ISO/SOC2) with minor security incidents, or a lack of documented AI security and privacy policy.	
		Tier 3 Standard validated controls, no known incidents, and basic AI disclosure or usage policies in place.	
		Tier 4 & 5 Strong, proactive posture with independent validation and mature AI safety and ethics frameworks.	

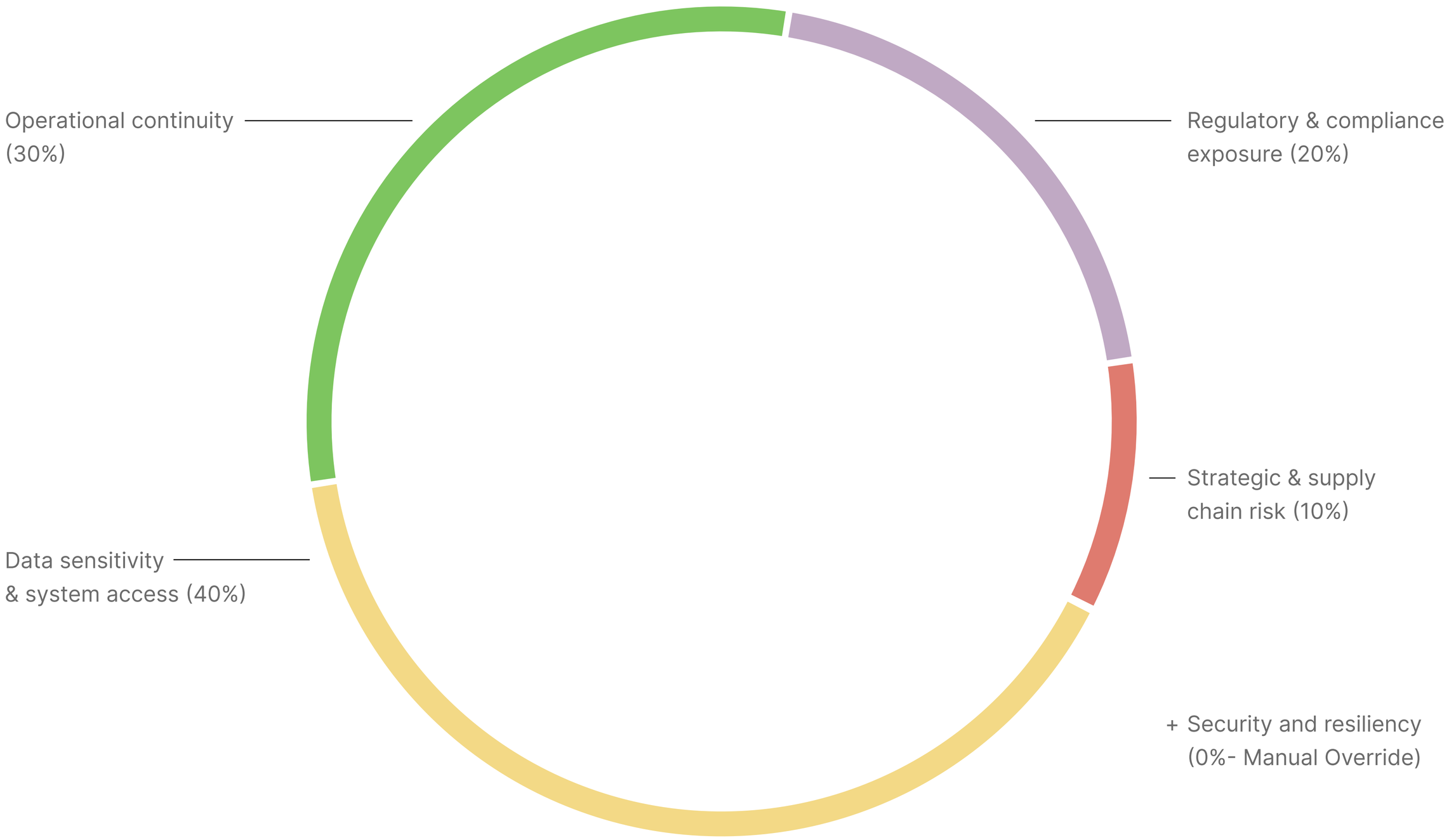
The methodology of weighting

Once you've aligned on your risk categories, applying a weighted scoring model can move you from information gathering to establishing objective tiers.

This prevents vendors from being tiered based on a single variable while ignoring others, keeping your focus on the drivers of real risk.

1. The Weight of Influence

In a defensible program, not all domains carry the same "weight" in the final calculation. For example, you could weight your risk categories as:



- **Operational continuity (30%):** Measures the business impact of a service outage and the organization's tolerance for downtime.
- **Data sensitivity & system access (40%):** The primary driver of cyber risk, evaluating the classification of data handled and the level of system access granted.
- **Regulatory & compliance exposure (20%):** Accounts for legal and contractual obligations tied to the vendor's specific function.
- **Strategic & supply chain risk (10%):** Long-term impact of vendor substitutability, geographic jurisdiction, and fourth-party concentration to prevent over-reliance on a single provider or region.
- \+ **Security and resiliency (0%- Manual Override):** Functioning as a binary gatekeeper rather than a score, this allows InfoSec to trigger a manual "block" if a vendor fails to meet baseline resilience or assurance standards.

2. The "Critical Trigger" override

While weighting provides a balanced view of most vendors, certain risk factors are so significant that they demand immediate escalation. This Override Logic acts as a strategic safety net. If a vendor meets any Tier 1 Indicator (such as handling millions of customer records or being a sole-source provider for a mission-critical process), they are automatically classified as Tier 1, regardless of their scores in other domains.

By applying this override alongside the weighted average, you can make sure that extreme, high-impact risks are prioritized and never “averaged out” or diluted by lower scores in secondary categories.

We recommend implementing both Tier 1 and Tier 2 override triggers within your tiering methodology to enable automatic escalation in response to critical risk conditions.

Defining vendor tiers (Critical to Transactional)

Now that you have defined risk categories and a scoring methodology, the next step is applying them through a structured, scorable framework. By evaluating vendors across each category and weighting results based on exposure and potential impact, organizations can derive an objective risk score. That score provides a clear, consistent basis for grouping vendors into tiers, ensuring critical relationships are reliably distinguished from moderate and lower-risk ones. This is what allows vendor tiering to scale while remaining defensible and repeatable.

While there is no universal rule for the number of tiers a program should have, the most resilient organizations recognize that granularity is key to scaling efforts appropriately. Organizations managing 200+ vendors typically benefit from a 5-tier model, which provides the nuance needed to differentiate levels of criticality at scale. Smaller organizations, or those managing fewer than 200 total vendors, may find a simpler 3-tier model sufficient.

In both cases, the objective remains the same. Eliminate complexity by distinguishing between critical vendors and moderate ones, and separating them from lower-risk or transactional vendors within your ecosystem.

In this Best-Practices Guide, we present a tiering model structured into five distinct tiers.

Tier 1 – Critical Vendors

Tier 1 vendors are absolutely vital to your operations, security, and their failure or compromise could result in significant operational disruption, impact, or regulatory exposure. These vendors support your mission-critical functions, handling your most sensitive data and/or are tightly integrated into your key products/services.

They could have a direct correlation to revenue generation and your customer-facing operations. The risk tolerance for Tier 1 is extremely low, requiring strong controls and resilient contingency plans built for these relationships.

Best practice

As Tier 1 vendors pose the highest risk, thorough due diligence and ongoing oversight are required. Best practices for Tier 1 include, at a minimum, annual comprehensive risk assessments (or more frequently, such as semi-annually), independent assessment evidence of the vendor's security and business continuity controls, and continuous monitoring to catch risks between assessments.

Essentially, Tier 1 vendors are treated as an extension of your enterprise. You must manage their risk almost as if they were an internal department.

Tier 1 vendors are typically your cloud infrastructure providers, primary payment processing gateways, confidential client data managers, and strategic outsourcing partners. Tier 1s are your core providers, critical to your business continuity.

Tier 2 – High-Risk Vendors

Your Tier 2 vendors are considered a substantial risk. They are essential to operations and can have a significant impact if they fail. Though not quite as indispensable as Tier 1, they typically carry moderate to high inherent risk.

Failures or breaches involving Tier 2 vendors can be costly, but may be contained or mitigated by firm contingency plans. They require close oversight, but not as intensively as Tier 1.

Risk tolerance for Tier 2 remains low but distinct from the 'very low' threshold of Tier 1, allowing organizations to actively manage and mitigate risks.

Best practice

Your Tier 2 vendors should receive regular risk assessments and oversight, with a lower level of intensity than Tier 1. For instance, you might review Tier 2 vendors annually or every two years. For good measure, ongoing monitoring should still occur. Many organizations treat Tier 2 as “critical” in a broad sense, just a notch below Tier 1 – so it still receives substantial management attention. The key difference is often in the frequency and depth of reviews.

Tier 2 vendors are your service providers that support your high-value systems but do not operate them end-to-end. Take an IT services provider, a significant marketing platform, a regional payroll provider, or a payment processor. Tier 2 vendors are substantial if they fail, but are not critical infrastructure within your ecosystem.

Tier 3 – Medium-Risk Vendors

Your Tier 3 vendors present a moderate or medium level of risk, providing essential goods or services, and are necessary for smooth business operations. The impact of an issue stemming from a Tier 3 vendor, while noticeable, would still be manageable without severe and costly long-term consequences.

These are your “standard” vendors, important for functionality but not critical to continuity. They have a limited scope of impact, causing inconveniences or minor financial effects but not widespread disruption. Here, risk tolerance is moderate, meaning you still want to mitigate risks but can tolerate some without significant damage.

Best practice

For Tier 3, a balanced approach is used. You’ll still perform due diligence and risk assessment, but less frequently – perhaps every two years, or during contract renewal cycles. Initial onboarding checks are done, and if they pass, ongoing oversight might be minimal. Continuous monitoring is recommended, but notification thresholds (i.e., score changes) could be more lenient.

One common practice is for business owners to attest annually that Tier 3 vendors are still being utilized as expected and haven’t assumed more critical activities. If a Tier 3 vendor starts taking on a more important role (e.g., expanding to handle more data or assuming a bigger role), you would re-evaluate and possibly bump them to a higher tier. In summary, Tier 3 vendors are managed with routine oversight. Enough to catch red flags, but not with the same intense scrutiny reserved for higher tiers.

Tier 3 vendors are necessary for daily business, such as an internal learning management system or an office supplies provider. Vendors in this tier may provide cloud software or plugins for your non-critical processes. These are valuable, but not essential, as their failure would cause inconvenience rather than disaster.

Tier 4 – Low-Risk Vendors

Your Tier 4 vendors pose minimal inherent risk and are not critical to business operations. These vendors provide non-essential goods and services and have very limited or no involvement in sensitive processes. Failures that have a lower impact on your organization are much easier to contain because these vendors are “low impact, low criticality”.

The risk tolerance for Tier 4 is high because organizations are comfortable accepting modest risk, which they can address with basic controls.

Best practice

Tier 4 vendors require only basic vendor management hygiene. Typically, you conduct initial due diligence during onboarding. After that, ongoing assessments are minimal, and you might not review them again unless something changes.

It’s common to simply track Tier 4 vendors in your vendor inventory and set a review every few years or at contract renewal to make sure nothing has changed on their end. Many organizations use a passive monitoring approach, taking action only if a Tier 4 vendor reports a significant issue or an obvious red flag appears. Otherwise, these vendors get light oversight.

Internally, it’s wise to have an exit strategy even for low-risk vendors, since they are easily replaceable, so no accidental dependency is created by neglecting alternatives. Tier 4 management is about keeping records and ensuring that no Tier 4 vendor “creeps” into a higher risk activity without being reclassified. Take a cleaning service, for example, categorized as a Tier 4 vendor, that starts handling badge printing (which may involve personal data/ photos). You may need to reevaluate their tier.

Tier 4 vendors pose low risk and can be replaced quickly if needed. Their relationship to your business continuity and success is marginal. It includes the likes of catering services, facility maintenance companies, cleaning services, office furniture, and scheduling tools for corporate volunteer events.

Tier 5 – Minimal-Risk Vendors

Tier 5 is the lowest risk category, encompassing your purely transactional, one-time, or low-value relationships. These vendors pose virtually no material risk to your organization and may be used for single or ad-hoc transactions, with no persistent access to systems or data.

Many organizations do not separate Tier 4 and Tier 5, but we have added a classification to explicitly identify vendors that require minimal risk management beyond standard procurement controls. These vendors have an extremely high risk tolerance, meaning organizations accept these engagements as routine transactions that do not warrant ongoing oversight.

Best practice

Tier 5 vendors typically follow simplified procedures and may be excluded from formal risk assessments if they are true one-offs. Due diligence is often unnecessary or limited to a review of the vendor's external attack surface for indicative references. Periodic reviews are not required because these vendors are maintained in the vendor inventory for record-keeping purposes, and risk management reviews occur only when the relationship changes.

It is crucial to have a process to reclassify a Tier 5 vendor to a higher tier when its scope expands. For instance, if a freelance IT consultant initially hired for a one-time task is later engaged for larger projects with system access, their tier should be reassessed. As long as vendors remain transactional and low-risk, minimal governance is sufficient.

Tier 5 vendors include the likes of one-time freelance services (e.g., translators or graphic designers), local florists that supply flowers, online retailers that sell office electronics, or a training workshop facilitator. These transactional vendors provide low-value, non-critical goods and services, with a primary focus on cost and efficiency, through routine procurement transactions rather than via the intensive vendor risk process.

Note: The distinction between Tier 4 and Tier 5 can blur across organizations. You may choose to maintain only four tiers and treat transactional vendors as "Low Risk." However, in organizations with huge vendor populations, having a Tier 5 helps filter out the noise, and you might exclude Tier 5 vendors from the formal TPCRM program beyond initial classification. This frees up your risk managers to focus on Tier 1-4. Make sure whatever tiers you use are well-defined and understood by all stakeholders.

The quantitative bridge

To apply this methodology in practice, consistently capture these inputs during vendor onboarding (intake) using a structured questionnaire completed by internal business owners and reviewed by InfoSec. An example onboarding questionnaire, built from the outlined risk criteria, is included in the appendix. By mapping the weighted scores from this intake process to the following tiers, you can define the appropriate level of oversight, assessment depth, and review frequency for each vendor.

Tier	Weighted Score (0-100)	Profile Summary	Risk Assessment Frequency	Override Triggers	Continuous Monitoring
Tier 1: Critical	80–100	Mission-critical to operations or security, with high-impact failure potential and/or access to highly sensitive or regulated data.	At onboarding and every 6–12 months. Also, reassess after any incident, significant change, or contract renewal.	Handles regulated or highly sensitive data at scale, supports a mission-critical process, has direct administrative system access, or is indispensable.	Required
Tier 2: High-Risk	65–79	Essential and carries significant inherent risk, where disruption or compromise would cause major business or compliance impact, but is not existential.	At onboarding and annually thereafter, or sooner if scope, data exposure, or control environment changes.	Substantial customer-facing or reputational impact risk, or introduces elevated supply chain concentration dependencies.	Required
Tier 3: Medium-Risk	45–64	Important but replaceable, with moderate access.	At onboarding and every two years, or earlier if the vendor's role, data access, or risk profile increases.	N/A (Calculated by score)	Recommended
Tier 4: Low-Risk	25–44	Non-essential, with no sensitive data access, and substitutable.	At onboarding and every three years, or sooner if the scope, data access, or contract terms change.	N/A (Calculated by score)	Recommended
Tier 5: Trans-actional	0–24	Ad hoc or one-time, with no system access.	At onboarding only. Reassess only if vendor's exposure, scope, or usage changes materially.	N/A (Calculated by score)	Optional

Note: While point-in-time assessments provide a snapshot of risk, continuous monitoring allows for real-time visibility into a vendor's security posture between assessment cycles. Effectively scaling this level of oversight across a large vendor ecosystem is only possible with dedicated technology.

Industry and regulatory considerations

Vendor tiering should reflect more than just technical risk. Your industry, regulatory obligations, and contractual requirements may require certain vendors to be treated as higher tier, even if their inherent cyber exposure appears moderate. These modifiers ensure your tiering approach remains defensible, compliant, and aligned to real-world business impact.

By incorporating these considerations, organizations can apply tiering consistently at scale while maintaining a clear, auditable rationale for prioritizing third-party oversight.

Regulated sectors

Align upper tiers with any “critical” or “material” vendor definitions required by your regulator.

Framework alignment

Scale assessment depth by tier using recognized standards such as NIST CSF, ISO 27001, or SIG.

Legal and data obligations

Elevate vendors handling regulated or sensitive data (for example, GDPR, HIPAA, or PCI DSS) to ensure appropriate scrutiny and oversight.

Concentration risk

Account for geographic, systemic, or fourth-party dependencies that could amplify disruption if a vendor fails.

Emerging AI risk

Assess the impact of AI when a vendor offers AI-native services or integrates AI features into existing tools. The use of large language models and automated processing introduces unique data, privacy, security, and ethical considerations, which may require assigning a higher risk level to maintain proper governance.

Contractual expectations

Use tiering to demonstrate proportionate oversight required by enterprise customers, regulators, or public-sector clients.

Do you know which vendors would bring your operations to a halt if they went down? How differently do you treat these from other vendors in your ecosystem?

How to implement vendor tiering – step by step

By reducing the administrative load on your InfoSec team, you can focus on strategy and translating this theory into a repeatable, auditable process that applies to building a new program from scratch or refining your current one. Use the following steps to turn your tiering framework from theory into a functional program:

1. Formalize your vendor tiering framework

Before applying tiering across your vendor ecosystem, it's good governance to formally agree on how tiering decisions will be made. This may be the framework outlined earlier, or a variation tailored to your organization's risk appetite, regulatory environment, and operating model.

Secure alignment and sign-off from leadership, GRC teams, or other relevant business stakeholders, and document the agreed approach. This creates a defensible record of how vendors are tiered and ensures that decisions are understandable, repeatable, and auditable over time.

Where possible, operationalize the framework by embedding it into vendor onboarding and review workflows. Updating intake forms, questionnaires, and risk assessment tools to reflect the approved criteria and scoring logic helps standardize data collection, reduce manual judgment, and support automation as the program scales.

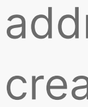
Tip: Tools like UpGuard can help operationalize your tiering framework by embedding approved criteria and scoring logic directly into vendor onboarding and review workflows. This makes capturing the right information for new vendors simple, consistent, and automated, reducing manual effort while maintaining governance and auditability.

■

2. Build a complete vendor inventory

You can’t tier what you can’t see. The first step is to build a complete, authoritative inventory of every third-party your organization relies on. To get started:

- Partner with Finance and Procurement to identify vendors with active or recent purchase orders, invoices, or contracts.
- Work with IT teams to surface vendors with system access, integrations or SaaS accounts that may sit outside formal procurement.
- Run a short internal survey asking business teams to list any vendors they rely on, including SaaS tools, consultants, and outsourced services.



Tip: Vendors like UpGuard can uncover relationships and exposures that traditional vendor lists miss. For instance, UpGuard’s User Risk detects shadow SaaS and unsanctioned applications in use across your environment. Vendor Risk identifies fourth-party dependencies and concentration risk, and Breach Risk highlights software products observed on domains or IP addresses. Together, these insights create a more complete view of your third-party ecosystem.

3. Assess and classify vendors

With your vendor inventory and tiering framework in place, the next step is to gather the information needed to apply them. Start by collecting available inputs internally across security, IT, procurement, and the business, such as system access, data handling, integrations, and operational dependency. If available, collect additional supporting evidence, such as contracts and vendor security evidence already provided. The example questionnaire in the appendix provides a practical starting point for collating the vendor information needed to support tiering decisions.

Apply the agreed scoring logic to these inputs to derive a risk score and assign each vendor to a tier. This initial tiering establishes a clear view of your third-party risk landscape and enables prioritization of follow-up actions and deeper assessment where required.

As additional information becomes available, tiers can be refined to reflect changes in exposure or vendor relationships.

Tip: Tools like UpGuard help centralise vendor information in a single, structured system of record. By consolidating inputs, evidence, and tiering decisions in one place, teams can maintain consistency, data integrity, reduce duplication, and make it easier to review, update, and defend vendor classifications over time.

4. Validate and share the results

Document final tiers in your vendor management system/record and share them with relevant stakeholders. High-risk and critical tiers must be reviewed, approved, visible, and sanctioned to be effective across the organization. TPCRM isn't owned solely by security; it's a shared operational dependency. If the business doesn't understand which vendors are critical or high risk, tiering becomes a back-office exercise rather than something that influences real decisions.

If a tier is adjusted manually, document the justification to maintain program defensibility.

■

5. Apply tier-based oversight

Oversight and effort are proportionate to risk—neither excessive nor insufficient. Use tiering to determine how your InfoSec team manages each vendor throughout its lifecycle:

- Align clauses and SLAs to risk (e.g., breach notification, audit/assessment rights, termination rights).
- Tailor assessment depth by tier during the onboarding assessment. Tools like UpGuard provide OoTB (Out-of-The-Box) assessment templates aligned with vendor tiers to reduce vendor fatigue and prevent over- or under-assessment.
- Review frequency based on tier (see Appendix A) with ongoing risk assessments.
- Establish continuous monitoring coverage for relevant vendor tiers.
- Assign ownership, for instance, Tier 1 vendors should have senior oversight, while lower tiers may sit within business units.

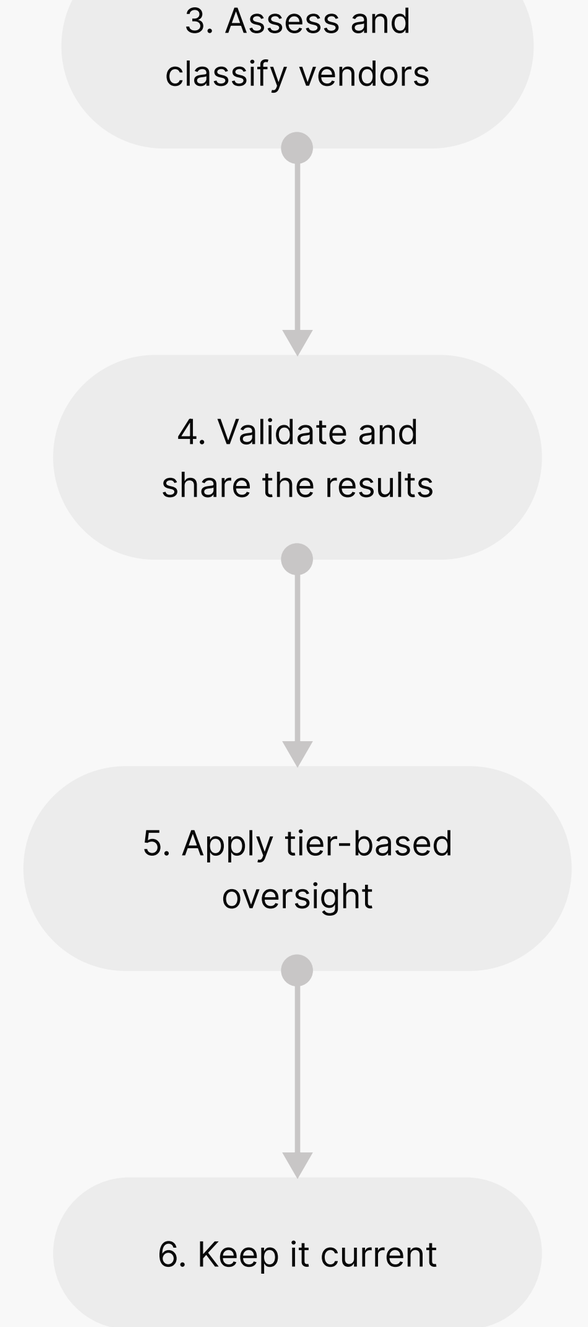
6. Keep it current

Tiering is not a one-off task. It is a program that must be applied consistently to provide focus, defensibility, and efficiency—not a static policy. Instead, it needs to remain accurate, relevant, and scalable as your business grows. Reassess a vendor's tiering:

- Annually or at renewal
- After significant changes, such as new data processing, incidents, or compliance shifts
- When usage or criticality increases

Review the overall tier distribution regularly. If too many vendors sit in upper tiers, refine your criteria, add more tiers (if using the three-tier model), or rationalize your vendor base.

How to implement vendor tiering flowchart



Now that you've built your tiers, you're ready to scale. Stay tuned for our insights on how to mature your program.

Own the risk, reclaim your strategic focus

Vendor tiering provides a practical foundation for scaling TPCRM. It helps teams focus oversight where it matters most, apply proportionate expectations across vendors, and make defensible, risk-based decisions as ecosystems grow. The most effective programs are built through steady progress, not overnight overhauls.

As your program matures, keep these three markers in mind:

- Recalibrate: Periodically revisit your tiering criteria, scoring logic, and tier definitions to ensure they still reflect your vendor ecosystem and the evolving threat landscape.
- Review: Reassess critical vendor tiers annually and others at key lifecycle moments, such as contract renewal, to confirm tiering remains accurate as relationships, exposure, and business dependencies change.
- Scale: If managing your vendor inventory, onboarding process, or assessments using spreadsheets or other manual methods starts to feel like a full-time job, that’s your cue to look into dedicated TPCRM technology.

Use the guidance in this eBook as a starting point, then work with your internal security, risk, and business stakeholders to validate and adapt the approach to your organization’s unique environment, risk appetite, and operational priorities.

With a clear framework in place and a commitment to continuous refinement, you can apply proportionate expectations across your entire vendor ecosystem and make defensible, risk-based decisions with absolute confidence.

Disclaimer: This guide presents general best practices and example criteria based on industry standards. It is intended to assist in developing your own internal procedures. It does not constitute legal advice or guarantee compliance with any specific regulation. Organizations should consult their compliance, legal, and risk professionals to ensure that their third-party risk management program – including vendor tiering – meets all applicable requirements and is tailored to their specific risk profile. Always document your decisions and be ready to show that your approach is reasonable and risk-based. When in doubt, err on the side of caution: it’s better to classify a vendor as higher risk and manage them accordingly than to underestimate a risk and face a potential incident unprepared. By following the guidance in this document and adjusting it to your needs, you will be well on your way to building a robust TPCRM that can confidently handle a large vendor ecosystem. Vendor tiering is a powerful tool – use it wisely, keep it updated, and it will pay dividends in reduced risk and improved operational resilience for your organization.

Appendix: Tiering framework resource

This appendix provides the foundational structure for categorizing and managing third-party risk. This resource ensures that vendor oversight remains proportionate, defensible, and aligned with your organization's risk appetite.

The onboarding questionnaire (intake form)

The first step in any tiering process is the collection of relationship context. Before a security assessment is sent, the business owner should complete a short internal questionnaire to define the vendor's profile. This data serves as the raw input for the Scoring Matrix and Override Triggers outlined in this guide. An example of an internal vendor onboarding questionnaire based on the risk criteria outlined in this eBook is below:

For business user completion:

Onboarding questions	Response questions
1. Basic vendor details	
Vendor name:	.....
Vendor website:	.....
Description of product/service:	.....
Primary contact/relationship owner:	.....
Annual contract value:	.....
Approximate annual spend or value of this engagement:	☐ <$10k ☐ $10–100k ☐ $100–500k ☐ >$500k
What is the contract renewal frequency?	☐ Annual ☐ Semi-Annual ☐ Quarterly ☐ Monthly ☐ Once-Off/Unknown ☐ Other
2. Service importance (operational criticality)	
If this vendor were unavailable for 24 hours, what would be the impact on your team's ability to operate?	☐ No impact ☐ Minor inconvenience ☐ Moderate disruption ☐ Major disruption ☐ Business stops completely
What is the maximum duration of a service outage that can be tolerated?	☐ Less than 1 hour ☐ 1 - 4 hours ☐ Up to 24 hours ☐ 2 - 4 days ☐ 1 week or more
Is there another vendor or internal process that could perform the same function if this one fails?	☐ Easily replaceable ☐ Some effort ☐ Difficult ☐ Not replaceable
Does this vendor support any services provided to our customers?	☐ No ☐ Yes, internal support only ☐ Yes, directly visible to customers
How difficult or time-consuming would it be to switch vendors?	☐ <1 month ☐ 1–3 months ☐ 3–6 months ☐ >6 months

Onboarding questions	Response questions
3. Data and access (data sensitivity & access level)	
What type of data will the vendor handle?	☐ None ☐ Public ☐ Internal business data ☐ Confidential (employee or company) ☐ Regulated/Sensitive (customer PII, PHI, card data, etc.)
What level of access will the vendor have to company systems or data?	☐ No access ☐ Read-only access ☐ Standard user/service access ☐ Privileged or administrative access
Will the vendor require technical integration or persistent connectivity into internal systems?	☐ No integration ☐ Basic integration only (e.g. SSO login or limited API connection) ☐ Ongoing system integration ☐ Direct network or remote access
Will the vendor host or store any company data in their own systems?	☐ No ☐ Yes (non-sensitive) ☐ Yes (sensitive)
4. Regulatory & compliance	
Does this vendor support or affect any regulated activities (e.g., financial reporting, personal data processing, safety, or compliance functions)?	☐ No ☐ Possibly/minor ☐ Yes – significant impact
Does the vendor help you meet a legal, contractual, or customer requirement?	☐ No ☐ Yes, indirectly ☐ Yes, directly required
5. Strategic risk	
Does this service act as a dependency for other systems, or require data exchange with existing applications?	☐ Isolated (no integrations) ☐ Minor (Integrates 1-2 non-critical tools) ☐ Moderate (Integrates with core productivity suites) ☐ Completely Integrated (Critical exchange with core business systems)
Would non-performance by this vendor result in financial penalties, loss of revenue, or breach of contract?	☐ No ☐ Possibly minor ☐ Yes, significant loss
Does the vendor rely on another key provider (e.g., a cloud hosting provider or a subcontractor) to deliver its service?	☐ No ☐ Yes/unknown
Where is the vendor headquartered, or where will data be processed/stored?	☐ Domestic/low-risk region ☐ Mixed/moderate risk ☐ High-risk/restricted region

■

For infosec completion:

Onboarding questions	Response questions
6. Security & resilience	
Does the vendor hold any recognised security certifications (e.g., ISO 27001, SOC 2, PCI DSS)?	☐ Yes, valid in the last 12 months ☐ Yes, but outdated ☐ None/unknown
Was the vendor involved in previous data breaches, outages, or major incidents involving this vendor in the past two years?	☐ No ☐ Minor issue ☐ Significant/multiple issues
Will this vendor use AI to process, analyse, or generate outputs using company or customer data as part of the service?	☐ No AI functionality ☐ AI is used, but not on our data ☐ AI is used on our data ☐ Unsure/vendor has not clearly confirmed
Can any company or customer data shared with this vendor be used to train, improve, or fine-tune their AI models?	☐ No ☐ Yes ☐ Unknown/not addressed by the vendor

Vendor Risk Powered by UpGuard

Ready to Scale With Absolute Visibility?

UpGuard’s new onboarding portal makes it easy for InfoSec teams to modernize their vendor intake and collect critical relationship data needed for a defensible TPCRM. By automating initial risk scores and deploying assessment templates perfectly aligned with a specific vendor’s profile, you can scale oversight in proportion without manual effort.

Book a demo →