The Definitive Third Party Risk Management Maturity Journey:

A Strategic TPRM Maturity Framework

SURECLOUD®

www.surecloud.com

SURECLOUD®

GDPR Compliant

teiss Awards Winner Best Security Compliance Product

Table of Contents

Highlights

- A seven stage maturity model for assessing current and target TPRM capability
- Practical guidance across vendor inventory, tiering, due diligence, governance, automation, reporting, and continuous monitoring
- A strategic framework for moving from reactive vendor oversight to integrated and continuously informed third party risk governance

Who should read this?

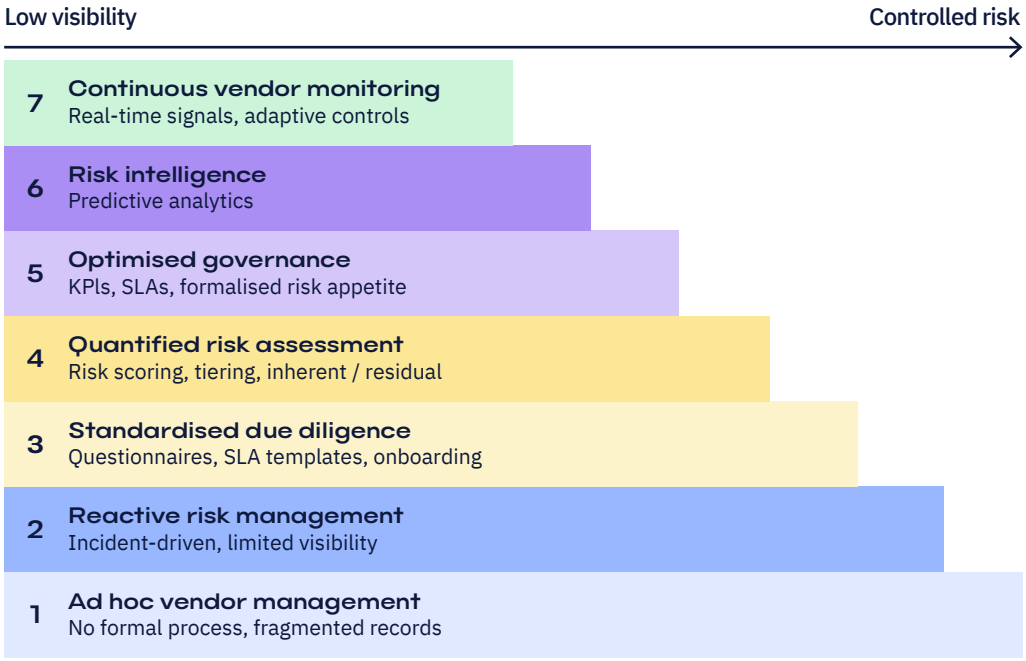
This guide is designed for senior leaders responsible for third party risk, cyber governance, compliance, and resilience, including CISOs, Heads of Third Party Risk Management, Vendor Risk Leaders, Heads of Risk and Compliance, Supply Chain Risk Leaders, and Internal Audit Directors.

It is also relevant for vendor risk analysts, IT security governance teams, procurement leadership, and data protection and privacy leaders involved in improving third party risk oversight across the organisation.

What this guide helps readers do

This guide helps readers assess current TPRM maturity, understand the operating model weaknesses that limit visibility and control, and identify the next practical steps most likely to improve governance, resilience, and oversight quality.

It also provides a structured way to evaluate how vendor inventory, tiering, due diligence, reporting, and technology need to evolve as third party ecosystems become more complex, more business critical, and more exposed to cyber, resilience, and regulatory risk.



1. Executive Summary

Third party risk management is no longer a narrow procurement or compliance activity. In 2026, it is a strategic capability shaped by the expansion of third party ecosystems, growing dependence on suppliers and technology providers, rising cyber supply chain risk, and stronger regulatory expectations around vendor governance. As third party relationships become more deeply embedded in operational and digital infrastructure, the risks associated with those relationships become more consequential for cyber security, resilience, regulatory compliance, and executive accountability.[1][2][3]

Many organisations have not adapted their operating model to match this reality. Third party risk programmes are still often built around spreadsheets, incomplete inventories, manual questionnaires, and periodic assessments that provide only limited visibility into changing vendor risk. In that environment, oversight remains fragmented, assurance remains inconsistent, and organisations are left reacting to issues rather than identifying them early.[1]

This is why TPRM maturity matters. A mature programme does more than document suppliers and complete due diligence. It builds a structured, risk based approach to vendor oversight across the full lifecycle of third party relationships. As programmes mature, they move from inconsistent tracking and one time assessments towards centralised inventories, risk based tiering, automated assessments, and more continuous monitoring of vendor risk.[1][6]

This guide presents TPRM maturity as a capability journey. It is designed to help organisations assess where they are today, understand the risks of remaining there, and identify the next capabilities needed to progress. Third party risk is now a major enterprise risk, and reactive vendor management is no longer sufficient. Organisations need a more integrated, risk led, and continuously informed approach if they want to manage supplier exposure with the level of confidence that 2026 demands.[1][2][3]

2. The Modern Third Party Risk Landscape

Third party risk is no longer a peripheral procurement concern. In 2026, it is part of the core enterprise risk environment because organisations now depend heavily on vendors, service providers, software platforms, cloud providers, and specialist partners that are embedded across digital operations, supply chains, customer delivery, and regulatory obligations. As those relationships become more business critical, the risk created by them becomes harder to isolate and harder to manage through static oversight alone.[14]

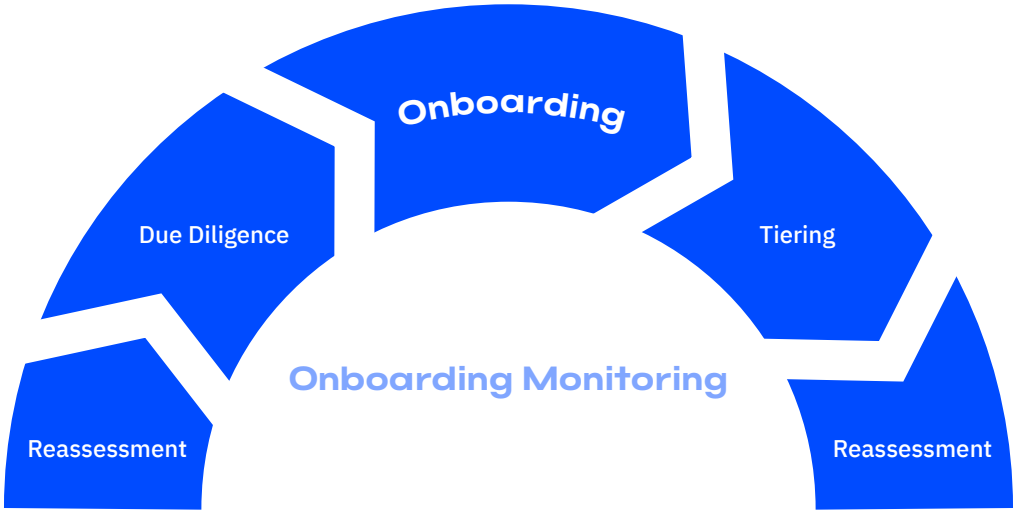
That shift is being driven by the scale and complexity of modern third party ecosystems. Many organisations rely on large numbers of suppliers across technology, operations, compliance, data processing, logistics, and specialist services. The challenge does not stop with direct suppliers. Fourth party exposure has become more material as critical vendors depend on sub processors, cloud hosts, software components, and outsourced providers that may be outside direct contractual visibility but still capable of creating disruption. Third party risk therefore needs to be managed as a lifecycle governance issue rather than a one time onboarding exercise.[4]

Cyber risk has made this landscape significantly more urgent. Third parties have become a common attack path because they can provide indirect access to systems, data, operational processes, and customer environments. A third party weakness is therefore rarely confined to the supplier itself. It can quickly become a customer outage, a resilience event, a data protection issue, a compliance failure, or a board level concern for the organisation that depends on that supplier. As supply chains become more digital and more interconnected, that exposure becomes harder to monitor through periodic assessment alone.[24]

Regulatory expectations are also rising. Third party governance is increasingly treated as part of wider operational resilience, cyber governance, and risk management rather than a narrow procurement discipline. In regulated sectors especially, the standard is shifting from showing that vendors were assessed at a point in time to showing that vendor risk is understood, tiered, governed, and monitored over the life of the relationship. Organisations are being asked not only whether they review third parties, but whether they can demonstrate proportionate and ongoing oversight.[35]

This is why third party risk now matters at executive and board level. The issue is no longer limited to supplier due diligence. It is whether the organisation understands where critical dependencies sit, how third party exposure affects resilience and compliance, and whether it has a defensible model for governing external risk across the full vendor lifecycle. Where that model is weak, leadership visibility is weak as well.[135]

The result is a more demanding third party risk environment: more dependence, more interconnected exposure, more regulatory scrutiny, and less tolerance for fragmented oversight. In that context, low maturity TPRM models built around spreadsheets, siloed ownership, and periodic assessments are becoming increasingly difficult to defend. Organisations need a more structured, risk led, and continuously informed approach if third party oversight is to keep pace with the realities of 2026.[145]



3. Why Third Party Risk Programmes Struggle

Many organisations recognise that third party risk has become more significant, but their operating model has not kept pace. That is why low maturity TPRM programmes often remain burdened by slow assessments, incomplete visibility, and fragmented accountability. The problem is not simply that the work is inefficient. The programme lacks the structure needed to give leadership a dependable view of vendor exposure across the organisation.[17]

One of the most common weaknesses is the vendor inventory itself. Many organisations still do not have a complete, governed view of their third party population, particularly where suppliers are onboarded through different business functions, systems, or procurement channels. That creates a visibility problem before any risk assessment begins. Programmes struggle to apply proportionate oversight if they cannot reliably identify which vendors exist, which services they support, what data they touch, or where material dependencies sit. Weak inventory quality then affects everything that follows, from tiering and due diligence to reassessment and reporting.[17]

A second weakness is the continued dependence on manual questionnaires, spreadsheets, and email driven coordination. These tools may appear workable at low scale, but they become increasingly inefficient as the number of vendors, assessments, remediation items, and reassessment cycles expands. Static questionnaires are especially limited because they often produce information that is already ageing by the time it is reviewed, and they rarely create the kind of reusable, comparable data needed for broader risk visibility. The result is more friction, more duplication, and less confidence in the consistency of oversight.[16]

A third issue is fragmented governance between procurement, risk, security, compliance, privacy, and the business. In lower maturity environments, procurement may manage the commercial relationship, while security or risk reviews the vendor from a control perspective, but without a shared governance model for ownership, escalation, and reporting. That creates inconsistent standards, duplicated requests, and weak accountability. It also makes it harder to distinguish between supplier administration and true third party risk governance. Where procurement and risk teams are not aligned, the organisation often struggles to apply consistent decisions across onboarding, reassessment, remediation, and exit.[79]

The final weakness is that many programmes remain reactive and audit driven. They mobilise when a new onboarding request appears, when an annual review becomes due, or when regulators, customers, or auditors request evidence. That kind of episodic effort may create the appearance of control, but it does not provide durable oversight across the vendor lifecycle. It also means the programme spends too much time responding to deadlines and too little time identifying changing risk early.[67]

Taken together, these are signs of a weak operating model, not just local process inefficiency. Inconsistent inventories weaken visibility. Manual assessment models reduce scale and comparability. Fragmented governance weakens accountability. Reactive review cycles weaken resilience and make assurance harder to defend. This is why many organisations remain stuck at low TPRM maturity even when they appear to be doing a large volume of work. The issue is not only effort. It is the absence of a more integrated and scalable model for governing third party risk across the full lifecycle. This is where the maturity model becomes useful.[167]

4. The Third Party Risk Management Maturity Model

The third party risk maturity model is the core framework of this guide because it translates the problems described in Section 3 into a practical way of assessing current capability and planning the next stage of improvement. Its purpose is to help organisations understand where their programme sits today, what risks are created by remaining there, and which capabilities need to be strengthened next. It does more than describe what good looks like. It also helps explain why vendor oversight remains fragmented, why assessments become burdensome, and why leadership visibility often remains weak even when organisations are doing a large volume of work.[1789]

This guide uses a seven stage model because it provides enough distinction to show meaningful development without becoming overly granular. Early stages are characterised by fragmented ownership, weak visibility, and static or inconsistent assessments. Later stages are defined by stronger governance, more targeted due diligence, automation, integrated risk visibility, and more continuous oversight. Progression is not simply a matter of adding more process. It depends on building a more coherent operating model for governing third party exposure across the full vendor lifecycle.[789]

Stage 1. Ad hoc vendor management

Characteristics

Third party risk activity is limited, inconsistent, and often handled within individual departments rather than as an enterprise capability. Vendors may be reviewed locally, but there is no common operating model, no defined governance structure, and little consistency in how risk is identified or documented. Oversight is typically reactive and driven by immediate business need rather than structured policy.

Operational risks

The organisation has little confidence that material third party exposures are being identified consistently. Blind spots are common, ownership is unclear, and vendors can be engaged without proportionate scrutiny.

Capabilities required to progress

Define the initial scope of the programme, establish named ownership, and begin creating a reliable inventory of third party relationships.

Stage 2. Basic vendor inventory

Characteristics

The organisation has begun to formalise its third party population through a register or inventory. Basic vendor information is captured, and some ownership starts to emerge. However, the inventory is often incomplete, updated manually, and not yet robust enough to support consistent governance decisions.

Operational risks

Incomplete or inconsistent inventory data makes it difficult to understand the full third party population, apply tiering, or target due diligence effectively. This weakens prioritisation and leaves material dependencies insufficiently visible.

Capabilities required to progress

Improve inventory quality, define baseline vendor attributes, and create enough data structure to support segmentation and assessment.

Stage 3. Structured due diligence

Characteristics

The organisation introduces more formal assessment methods. Third party due diligence becomes more repeatable, and questionnaires or reviews are used more consistently at onboarding or renewal. Vendors are increasingly assessed through a standard process rather than purely local judgement.

Operational risks

The programme can still remain slow, manual, and inconsistent if assessments are not tied clearly to risk level. Static questionnaires may create burden without producing a proportionate or reusable risk view.

Capabilities required to progress

Introduce risk based vendor tiering, make assessment methodologies more proportionate, and align review criteria more clearly to the nature of the third party relationship.

Stage 4. Centralised governance

Characteristics

Governance becomes more structured and more centralised. Ownership is clearer, standards are more consistent, and cross functional coordination improves between risk, procurement, security, compliance, and the business. TPRM begins to operate as a recognised governance process rather than a disconnected collection of checks.

Operational risks

Even with stronger governance, the programme can remain operationally inefficient if the inventory, due diligence process, and issue tracking still rely too heavily on manual activity. Governance can become more visible without becoming scalable.

Capabilities required to progress

Strengthen workflow discipline, improve issue management, and prepare for automation in assessment, tracking, and reporting.

Stage 5. Automated vendor assessments

Characteristics

The programme begins to reduce manual effort through more automated questionnaires, workflow orchestration, reminders, issue tracking, and evidence handling. Assessments become easier to manage at scale, and reassessment activity becomes more structured and repeatable.

Operational risks

Automation can improve efficiency without solving underlying fragmentation if vendor data, governance, and risk reporting are still disconnected. The programme may be faster, but not yet more integrated.

Capabilities required to progress

Connect assessment workflows to broader risk, compliance, and reporting structures so that vendor oversight becomes more decision useful across the organisation.

Stage 6. Integrated risk visibility

Characteristics

Third party risk information becomes more connected across the organisation. Vendor data, assessment results, remediation activity, external intelligence, and reporting are increasingly brought together into a more unified risk view. This supports stronger prioritisation, better escalation, and improved understanding of concentration and dependency risk.

Operational risks

Without more continuous oversight, integrated visibility can still remain too retrospective. The organisation may understand vendor exposure more clearly, but still react too slowly to change if monitoring triggers and lifecycle oversight remain limited.

Capabilities required to progress

Introduce more continuous vendor monitoring, event based reassessment triggers, and stronger lifecycle oversight across onboarding, review, incident response, and offboarding.

Stage 7. Continuous vendor monitoring

Characteristics

Third party risk management operates as a more mature, ongoing capability. The organisation maintains stronger lifecycle visibility, uses more continuous signals to monitor vendor risk, and is better able to identify changes in security posture, resilience, compliance exposure, or dependency risk over time. Reporting becomes more decision useful, and TPRM is better integrated with broader governance and resilience efforts.

Operational risks of remaining below this stage

Organisations that do not reach this level remain more dependent on point in time review cycles and are less able to detect emerging vendor risk before it becomes operational disruption, regulatory exposure, or executive concern.

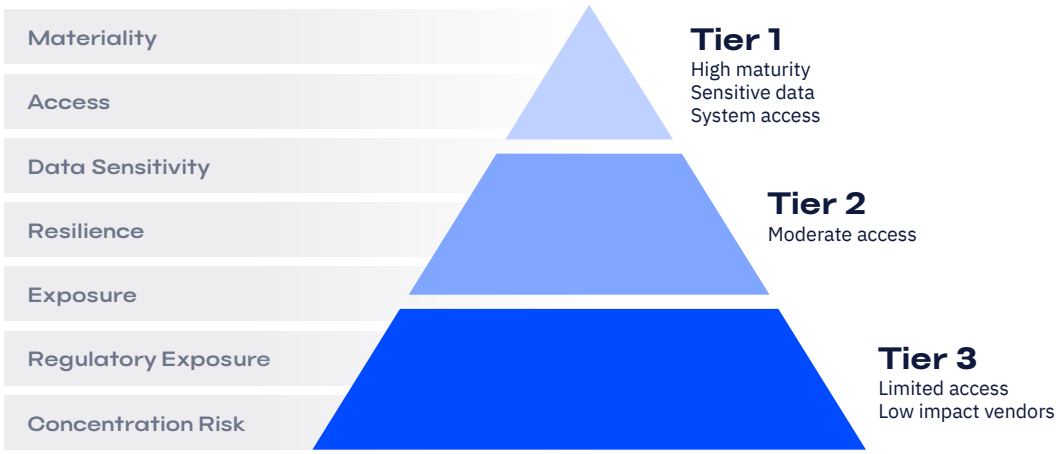
Capabilities required to sustain this stage

Disciplined governance, high quality vendor data, integrated workflows, continuous improvement, and the ability to turn monitoring signals into proportionate action and decision support.

Across all seven stages, the pattern is consistent. Lower maturity programmes are dominated by fragmented ownership, weak inventories, static assessments, and reactive oversight. Higher maturity programmes centralise governance, improve data quality, automate assessment activity, integrate risk visibility, and build towards more continuous vendor monitoring. This is what allows TPRM to evolve from a periodic control exercise into a more strategic and resilient risk capability. The model helps organisations identify where they are, why they are there, what risks that creates, and which capabilities will make the next stage of progress credible.[78]

5. What Mature TPRM Programmes Look Like

Mature third party risk management becomes clearer when the higher stages are examined in practice. Mature third party risk management programmes do not simply complete more due diligence activity. They make third party oversight more proportionate, more visible, and more useful to decision makers. That is what distinguishes advanced programmes from lower maturity models that rely on static questionnaires, fragmented ownership, and periodic review cycles. Mature TPRM is best understood through four characteristics: risk based vendor segmentation, integrated risk and compliance frameworks, continuous monitoring, and centralised reporting. Taken together, these characteristics show how TPRM evolves from a control exercise into a stronger governance capability.[7][8]



The first characteristic is risk based vendor segmentation. Mature programmes do not treat all vendors as if they create the same level of exposure. They distinguish between relationships based on materiality, access, data sensitivity, resilience impact, regulatory exposure, and concentration risk, then align due diligence, reassessment cycles, monitoring intensity, and escalation thresholds accordingly. This makes oversight more proportionate and more scalable. It helps organisations focus attention where the exposure is highest rather than consuming equal effort across all third parties.[10]

The second characteristic is the use of integrated risk and compliance frameworks. Mature TPRM does not sit in isolation from procurement, cyber security, privacy, operational resilience, compliance, or enterprise risk management. Instead, it connects those functions through a more coherent governance model. That reduces duplication, improves consistency, and makes it easier to understand third party exposure in the context of wider business objectives and enterprise risk. For leadership, the value lies not only in better coordination, but in a clearer view of how vendor risk affects resilience, compliance, and decision making across the organisation.[8][9]

The third characteristic is continuous monitoring. Mature programmes move beyond static onboarding checks and annual reassessment cycles. They introduce more ongoing visibility into changes in vendor risk posture, including security posture, resilience indicators, concentration risk, remediation status, and other signals that suggest the exposure associated with a vendor relationship is changing. In practice, this allows TPRM to become more proactive. Rather than relying only on point in time review, the programme becomes better able to identify change early and respond before emerging risk turns into operational disruption, regulatory exposure, or executive concern. It is also one of the clearest signs that a programme has moved beyond static risk assessment towards more resilient oversight of vendor performance and security posture.[7][10]

The fourth characteristic is centralised reporting. Mature reporting does more than show how many vendors have been assessed. It gives leadership a usable view of where critical dependencies sit, which vendor groups carry elevated exposure, where remediation is stalling, and how third party risk connects to cyber security, resilience, compliance obligations, and operational continuity. That visibility is one of the main strategic advantages of maturity. It improves prioritisation, supports escalation, and gives decision makers more confidence in how external exposure is being governed.[9]

Taken together, these characteristics show that mature TPRM is not defined only by more process or more tooling. It is defined by stronger segmentation, better governance integration, more continuous oversight, and clearer reporting for decision makers. This is what enables organisations to move from fragmented vendor management towards more proactive and more resilient third party risk governance. The next question is how to move towards that state in practice.[7][8][9][10]

6. Building a Roadmap to TPRM Maturity

Maturity rarely comes from a single transformation initiative. It usually develops through a sequence of practical improvements that strengthen visibility, governance, and operating discipline over time. If the foundations are weak, later improvements such as automation and integrated reporting will be less reliable and less useful.[17]

The starting point is a stronger vendor inventory. Many organisations try to improve TPRM before they have a complete and governed view of which third parties they rely on, what services they provide, what data or systems they touch, and where critical dependencies sit. That makes every later stage of maturity harder. A roadmap should therefore begin by improving the completeness, consistency, and ownership of the vendor inventory so it can support segmentation, due diligence, reassessment, and reporting with greater confidence.[17]

Once the inventory is more dependable, the next step is to define risk based vendor tiers. This is what turns a list of suppliers into a more usable governance model. Mature programmes do not apply the same level of oversight to every vendor. They distinguish between relationships based on materiality, access, data sensitivity, resilience impact, regulatory exposure, and concentration risk, then align review intensity accordingly. This is why tiering sits directly after inventory maturity in the roadmap. Without a dependable inventory, tiering is weak. Without tiering, due diligence becomes inefficient and poorly targeted.[10]

The third step is to improve assessment methodologies. In lower maturity programmes, assessment often becomes a repetitive questionnaire exercise that is slow, burdensome, and only loosely connected to the real risk presented by the relationship. More mature programmes improve this by aligning assessment depth and methodology more clearly to vendor tier, service type, and risk profile. That means reducing unnecessary friction, improving comparability across vendors, and producing outputs that are more useful for follow up, remediation, and decision making. Stronger methodology turns tiering from a classification exercise into a practical oversight model.[6][10]

Only then does it make sense to introduce automation. Automation can reduce operational drag across questionnaires, reassessment workflows, evidence handling, reminders, issue tracking, and reporting, but it should not be treated as a shortcut to maturity. If inventory quality is poor, if tiering is inconsistent, or if assessment methodology is weak, automation will simply scale those weaknesses. The better sequence is to stabilise governance and operating foundations first, then automate the activities that create the most friction and the least strategic value when handled manually.[7]

Across all of this, governance ownership and cross functional collaboration are what hold the roadmap together. TPRM maturity depends on clearer ownership between procurement, security, compliance, privacy, resilience, legal, and business stakeholders, as well as a shared understanding of what the programme is trying to achieve. It also depends on improving the quality of the underlying data so that inventory, tiering, assessment, and reporting become more dependable over time.[7][8][9]

This is why the strongest roadmaps are incremental rather than overly ambitious. They sequence capability building in a way that reduces friction, strengthens accountability, and creates a more scalable basis for ongoing third party oversight. Inventory enables tiering. Tiering makes due diligence more proportionate. Better due diligence creates more decision useful outputs. Automation then helps the programme scale those foundations more effectively. That is the maturity pathway this section is intended to support.[6][7][10]

7. Technology as a TPRM Enabler

Technology should be understood as a TPRM enabler, not a substitute for maturity. The role of technology in this journey is not to create a programme where the foundations are weak. It is to help a maturing programme become more consistent, more scalable, and more visible across the third party lifecycle. This matters because TPRM maturity depends first on governance, inventory quality, risk tiering, and sound assessment methodology. Technology becomes most valuable once those foundations are strong enough to support it.[6][7]

The first area where technology helps is automated vendor questionnaires. In lower maturity environments, due diligence often depends on static spreadsheets, document chasing, and manual follow up across multiple teams. More mature technology can standardise questionnaire workflows, route assessments according to vendor tier, support response reuse where appropriate, and reduce duplicated effort across the lifecycle. The objective is not speed for its own sake. It is consistency, proportionality, and the ability to manage assessments at scale without relying on fragmented local coordination.[6][10]

A second area is workflow automation. TPRM programmes become difficult to sustain when onboarding, reassessment, remediation tracking, approvals, and escalation all depend on email coordination and siloed spreadsheets. Technology can improve this by structuring tasks across procurement, security, compliance, privacy, legal, and business stakeholders in a more disciplined way. That improves accountability, reduces avoidable delay, and creates a stronger record of how third party risk decisions are made over time. In maturity terms, workflow automation supports operating discipline. It does not replace governance.[7]

A third area is risk scoring. As vendor populations expand, organisations need a more structured way to prioritise attention and distinguish between low impact suppliers and relationships that create significant operational, cyber, data, or resilience exposure. Technology can support this by bringing together vendor data, assessment outputs, tiering logic, and monitoring inputs into a more coherent risk view. Used well, this helps the organisation focus effort where the exposure is highest rather than treating all vendors alike. The benefit is better prioritisation and better governance visibility, not simply more data.[10]

The fourth area is vendor dashboards and reporting. Mature TPRM programmes need more than a count of completed assessments. They need reporting that helps leadership understand inventory quality, tiering distribution, assessment coverage, remediation status, concentration risk, and where material vendor exposure is changing over time. Dashboards are useful when they make third party risk more decision useful across the organisation. Reporting maturity is not about visualisation alone. It is about whether leaders can use the information to prioritise action, strengthen oversight, and understand how third party exposure affects resilience and compliance.[17]

Technology does not create TPRM maturity on its own. If inventory data is incomplete, if governance is unclear, or if tiering and assessment methodology are weak, technology can simply make fragmented processes faster. Used in the right sequence, however, it helps organisations scale stronger foundations and move from static, manual oversight towards more integrated and more continuously informed third party risk management. That is why technology belongs in the maturity journey as an accelerator of capability rather than the starting point for it.[6][7][10]

8. Measuring TPRM Success

If TPRM maturity is a journey, organisations need a disciplined way to know whether they are genuinely progressing. Measurement should do more than show that activity is taking place. It should indicate whether the programme is becoming more scalable, more risk led, and more useful to governance and decision making. That is why mature TPRM programmes should be measured through indicators that reflect coverage, efficiency, visibility, and assurance readiness rather than raw process volume alone.[1789]

One important category of measurement is coverage. This includes the percentage of vendors risk assessed, but more importantly it includes whether critical and high risk vendors are being assessed consistently, whether tiering is applied reliably across the inventory, and whether reassessment coverage is aligned to current exposure. A large number of completed assessments may look positive, but it is less valuable than knowing whether the programme has dependable oversight of the relationships that matter most. In maturity terms, coverage is not about volume. It is about whether the organisation can demonstrate proportionate oversight across its third party population.[10]

A second category is efficiency and throughput. Time to complete vendor onboarding is a good example. In lower maturity environments, onboarding is often slowed by incomplete inventory information, repetitive questionnaires, unclear ownership, and fragmented review cycles. More mature programmes should be able to reduce this friction without weakening scrutiny. Speed alone is not the goal. The more important question is whether the programme can deliver proportionate due diligence in a more repeatable and scalable way. This is why onboarding time, reassessment throughput, and remediation cycle time are useful maturity indicators. They show whether the operating model is becoming easier to sustain under real business demand.[17]

A third category is risk visibility. Mature TPRM programmes should be able to show where critical dependencies sit, which vendor tiers carry elevated exposure, where remediation is overdue, and how third party risk is distributed across cyber security, resilience, compliance, privacy, and operational continuity. This is where measurement becomes strategically valuable. Better visibility improves prioritisation, supports escalation, and helps leadership understand where material exposure is concentrated. In that sense, visibility is not only a reporting outcome. It is one of the clearest signs that the programme is becoming more decision useful.[789]

A fourth category is assurance readiness. Reduction in audit preparation effort is a practical signal here. Lower maturity programmes often spend significant time gathering due diligence records, confirming ownership, reconciling vendor data, and assembling evidence for regulators, customers, or auditors. As maturity improves, that burden should decline because records are more complete, workflows are more consistent, and reporting is easier to produce. This matters because it links operating discipline directly to governance confidence. A programme that is more continuously ready is usually one that is also more mature, more coordinated, and easier to defend under scrutiny.[17]

Together, these measures provide a more balanced view of TPRM success. Coverage shows whether the programme is seeing enough of the vendor population. Efficiency shows whether due diligence and oversight are becoming more scalable. Visibility shows whether third party risk information is becoming more useful for prioritisation and oversight. Assurance readiness shows whether the programme is becoming easier to govern and defend. This kind of measurement model supports maturity progression rather than simply tracking activity for its own sake.[1789]

Stage 1: Initial *Adhoc*

Unstructured, reactive approach with no formal programme

- [ ] Third-party risks are addressed informally, only when an incident occurs
- [ ] No defined TPRM policy, process or ownership exists
- [ ] Vendor onboarding relies on individual judgement with no standard criteria
- [ ] Risk assessments are not documented or consistently performed
- [ ] No central inventory of third-party relationships is maintained
- [ ] Limited awareness of regulatory requirements related to third parties

Stage 2: Developing *Emerging*

Basic awareness exists; some pockets of activity but no consistency

- [ ] TPRM is recognised as important but remains largely siloed across teams
- [ ] Some vendor questionnaires or due diligence templates exist informally
- [ ] Risk ownership is unclear or informally assigned
- [ ] A partial vendor register may exist but is not actively maintained
- [ ] Risk assessments are performed for some vendors, driven by procurement needs
- [ ] Limited integration with the wider enterprise risk framework

Stage 3: Defined *Structured*

Formal programme established with documented policies and processesy

- [ ] A documented TPRM policy and framework has been approved and communicated
- [ ] Tiering or criticality classification applied to segment the vendor population
- [ ] Standard risk assessment methodology used consistently across vendor types
- [ ] A complete vendor inventory is maintained with defined data fields
- [ ] Clear ownership assigned; a TPRM function or dedicated roles exist
- [ ] Contractual minimum security requirements are defined and applied

Stage 4: Managed *Controlled*

Programme actively managed with metrics, monitoring and governance

- [ ] Risk assessments are regularly reviewed and updated on a defined cycle
- [ ] Ongoing monitoring (e.g. cyber ratings, news feeds) applied to critical vendors
- [ ] Key risk indicators and programme metrics reported to senior stakeholders
- [ ] Incident and breach notification obligations are contractually embedded
- [ ] Vendor performance and SLA adherence tracked alongside risk posture
- [ ] TPRM is integrated into procurement, legal and change management processes

Stage 5: Integrated *Embedded*

TPRM embedded across the organisation and supply chain

- [ ] Fourth-party (sub-contractor) risks are identified and assessed
- [ ] TPRM requirements flow consistently through supplier contracting and renewal
- [ ] Business units actively participate in vendor risk reviews, not just procurement
- [ ] Risk appetite statements inform vendor tier thresholds and treatment decisions
- [ ] Technology tooling supports workflow, tracking and reporting at scale
- [ ] Regulatory mapping ensures TPRM controls address specific obligations (DORA, etc.)

Stage 6: Advanced *Proactive*

Proactive, intelligence-led approach with continuous improvement

- [ ] Threat intelligence informs vendor risk prioritisation and reassessment triggers
- [ ] Concentration risk analysis performed to identify single points of dependency
- [ ] Scenario analysis and stress testing applied to critical third-party relationships
- [ ] Vendor risk data is enriched with external signals (breach databases, sanctions lists)
- [ ] TPRM outcomes are benchmarked against industry peers or frameworks (ISO 27036)
- [ ] Continuous assurance replaces point-in-time assessments for tier-one vendors

Stage 7: Optimised *Leading*

Industry-leading practice with innovation and ecosystem resilience

- [ ] TPRM programme is continuously refined using data analytics and lessons learned
- [ ] Collaborative assurance model in place (shared assessments, mutual audit rights)
- [ ] Resilience planning extends to multi-tier supply chain disruption scenarios
- [ ] TPRM outcomes directly influence strategic sourcing and vendor portfolio decisions
- [ ] Automation and AI-assisted tools reduce manual assessment burden significantly
- [ ] Organisation actively contributes to industry working groups or standards bodies

9. The Future of Third Party Risk Management

The future of third party risk management is not defined by longer questionnaires or more frequent periodic reviews. It is defined by how well organisations can turn third party oversight into a more continuous, intelligence led, and decision useful capability. This shift is strategic, not merely operational. As third party ecosystems become more complex and more deeply embedded in core business activity, organisations need a model of oversight that can identify change faster, prioritise response more effectively, and connect external exposure to broader resilience and governance decisions.[24811]

One of the clearest shifts is towards continuous vendor monitoring. Static onboarding assessments and annual reviews are becoming less sufficient on their own because vendor risk posture can change much more quickly than traditional review cycles can capture. Changes in security posture, dependency risk, financial stress, incidents, geopolitical exposure, or regulatory context can all alter third party risk between formal assessments. The future of TPRM therefore depends less on isolated review points and more on the ability to maintain ongoing visibility into material change over time.[211]

A second shift is the rise of real time risk intelligence. More mature TPRM models are increasingly shaped by event based insight rather than fixed review calendars alone. External signals, cyber intelligence, supplier change indicators, incident data, and concentration insights are becoming more important because they help organisations identify where exposure is changing in ways that warrant reassessment or escalation. As a result, TPRM becomes more responsive and more proportionate. Instead of treating all vendors as static risk objects, organisations can respond to change as it emerges.[211]

A third shift is AI assisted vendor assessment. This does not remove the need for governance or human judgement, but it is beginning to change how TPRM programmes handle scale. AI assisted workflows can help triage vendor responses, identify anomalies, prioritise remediation, and surface inconsistencies across assessments and documentation. Used carefully, AI is likely to become an important accelerator of efficiency and insight in vendor assessment rather than a replacement for risk ownership. Its value will be greatest where inventory quality, tiering logic, and assessment methodology are already mature enough to support more intelligent automation.[711]

The fourth shift is integrated cyber supply chain risk management. Third party risk is moving closer to cyber security, operational resilience, business continuity, data governance, and enterprise risk management rather than remaining a standalone vendor management discipline. This is partly because the same supplier can create exposure across multiple domains at once, and partly because the supply chain itself has become a major route through which cyber, resilience, and regulatory risks propagate. The future of TPRM is therefore likely to be less siloed, more interconnected, and more explicitly tied to enterprise resilience and governance.[248]

The strategic implication is not that every organisation needs to implement every advanced capability at once. It is that future readiness depends on the foundations built earlier in the maturity journey. Organisations with stronger inventories, better tiering, clearer governance, more consistent assessments, and integrated reporting will be much better positioned to adopt continuous monitoring, AI assisted oversight, and more responsive forms of third party risk intelligence. TPRM maturity remains the right organising model for this guide. The future will favour organisations that treat third party risk as a continuously governed enterprise capability rather than a periodic vendor review exercise.[811]

10. Building Stronger Third Party Risk Governance

Third party risk management maturity is not an abstract framework. It is a practical way for organisations to move from fragmented vendor oversight towards a more resilient, integrated, and continuously informed model of risk governance. That is the central message running through this guide. TPRM must now be treated as a strategic capability rather than a narrow compliance task.[17]

The challenge is no longer simply to assess vendors at onboarding or to complete due diligence for audit purposes. Modern organisations rely on suppliers, technology providers, and service partners that are deeply embedded in digital and operational infrastructure. That means third party exposure now has direct implications for cyber security, resilience, compliance, privacy, and executive accountability. Where TPRM remains immature, those dependencies are too often managed through inconsistent inventories, static assessments, manual coordination, and reactive review cycles.[1][2][3]

Maturity changes that picture. A more mature TPRM programme gives organisations stronger inventory visibility, more proportionate vendor tiering, better coordinated governance, more scalable assessments, and clearer reporting for decision makers. Over time, it helps shift the programme from periodic vendor oversight to proactive risk management that is better aligned with wider governance, resilience, and compliance priorities.[7][8][9][10]

Self assessment is the right starting point. Organisations should first identify which maturity stage most closely reflects their current operating model, where the biggest sources of friction and exposure sit, and which capabilities are most urgent to strengthen next. From there, the priority is to define a realistic roadmap: improve inventory quality, strengthen tiering, make assessment more proportionate, improve governance ownership, and introduce automation in the right sequence. The goal is not to transform everything at once. It is to make the next stage of progress credible and sustainable.[6][7]

Third party risk is now too significant, too connected, and too dynamic to be managed through fragmented and reactive processes alone. Organisations that invest in TPRM maturity will be better positioned to govern third party exposure with greater confidence, respond earlier to changing risk, and support stronger enterprise resilience over time. That is the value of the maturity journey: not a fixed destination, but a practical path towards more effective and more defensible third party risk governance.[11]

References

1. **PwC.** Global Compliance Survey 2025.
2. **ENISA.** ENISA Threat Landscape 2025.
3. **FINRA.** 2025 Annual Regulatory Oversight Report: Third-Party Risk Landscape.
4. **ENISA.** NIS Investments 2025: Main Report.
5. **ENISA.** Technical Implementation Guidance on Cybersecurity Risk Management Measures.
6. **ISACA.** Vendor Risk Assessments: Do Organizations Still Need Them?
7. **KPMG.** Achieving resilience in third-party risk management.
8. **National Institute of Standards and Technology.** Cybersecurity Framework 2.0: Enterprise Risk Management Quick-Start Guide NIST SP 1303, Initial Public Draft.
9. **National Institute of Standards and Technology.** Integrating Cybersecurity and Enterprise Risk Management (ERM).
10. **Gartner.** Third-Party Risk Management (TPRM): A Complete Guide.
11. **PwC.** Navigating the future of digital trust: Learning from PwC's Global Digital Trust Insights 2026.

For more information on how SureCloud can assist your organization, visit us online at **www.surecloud.com**, or email **sales@surecloud.com**

SureCloud Summary

SureCloud Ltd. has two decades of experience as a leading provider of Governance, Risk, and Compliance (GRC) solutions since its founding in 2006. Headquartered in the UK, with offices in the US, SureCloud supports a global portfolio of organisations with its holistic and intelligent GRC platform. Whether addressing cyber risk, data privacy, third parties, or compliance demands, SureCloud has a proven record of empowering organisations to continuously identify, manage and automate their risk and regulatory alignment.

Corporate Headquarters 1 Sherwood Street, London, W1D 7HR