

The GAN Integrity Guide to
**Third-Party Risk Management
Program Maturity**





Why Your TPRM Program Maturity Matters

Third-party relationships have never been more essential, or more exposed. As global supply chains expand, regulatory expectations multiply, and new risk domains emerge across anti-corruption, sanctions, ESG, human rights, data privacy, and cybersecurity, compliance teams face a defining challenge: how do they deliver robust, defensible due diligence at scale, with the visibility and speed that modern business requires?

The answer depends heavily on where your program stands today. According to GAN Integrity and Compliance Week data, most organizations are managing more third parties than ever (in some cases thousands) yet 52% of compliance teams operate with ten or fewer FTEs. The risk landscape is growing faster than the teams responsible for managing it, and traditional manual processes have already hit their limits.

Regulators are watching. The US Department of Justice's guidance for evaluating corporate compliance programs explicitly asks whether a program is *truly effective, resilient, and agile*, not merely whether a process exists on paper. The EU's Corporate Sustainability Due Diligence Directive (CSDDD) and Germany's Supply Chain Due Diligence Act raise expectations further, demanding transparency not just into direct vendors, but deep into multi-tier supply chains. Against this backdrop, a mature TPRM program is no longer simply a compliance safeguard. It is a visible signal of organizational integrity, a competitive advantage in contracting and talent, and an early warning system for operational and reputational risk.

Understanding where your program stands today (honestly and specifically) is the essential first step. That is what a maturity model provides. Not a judgment, but a map.

How to Move Up the Maturity Curve

Progress on the TPRM maturity curve does not require doing everything at once. The organizations that make the most sustained progress take a deliberate, phased approach — solving the most critical gaps first, building organizational confidence along the way, and letting data from an improving program guide the next move. There is a clear pattern to how leading compliance teams advance.

Start your inventory and workflow infrastructure

The single biggest accelerant at Phases 1 and 2 is establishing a centralized, searchable third-party inventory and replacing ad hoc processes with purpose-built technology. When vendors are easy to onboard, assessments are automatically triggered and routed, and all data lives in one place, the compliance team stops spending its time chasing responses and starts spending it on the relationships that actually require judgment.

Extend from point-in-time to continuous.

A one-time onboarding assessment is a snapshot. Risk happens continuously. Moving to year-round monitoring — where adverse media, sanctions changes, ownership shifts, and new risk signals are surfaced in real time — closes the gaps that periodic reviews leave open. This single change transforms TPRM from an administrative exercise into a genuine early warning mechanism.

Connect the data.

The most powerful step on the maturity journey is integrating TPRM data with adjacent compliance domains: conflicts of interest, gifts and entertainment, incident management, and internal investigations. When a vendor who appears in a TPRM screening also appears in an employee's undisclosed COI declaration, that connection is invisible in a siloed system. On an integrated platform, it becomes a signal your compliance team can act on proactively.

Use AI to predict, not just report

At the highest levels of maturity, TPRM programs shift from documenting what happened to anticipating what is likely to happen next. Risk-based triage, AI-powered screening that reduces false positives by up to 77%, and analytics that surface patterns across the third-party ecosystem allow compliance teams to allocate their attention where it matters most and to demonstrate program effectiveness to regulators and boards with confidence.

Each step forward delivers compounding value. The model below maps that journey across five distinct phases. Use it to identify where your program sits today, understand the risks that come with staying there, and see clearly what the path forward looks like.



The Five Phases of TPRM Program Maturity





PHASE 1 OF 5

Informal

"We have a list of vendors. Somewhere."

WHAT IT LOOKS LIKE:

Third-party risk management exists on paper — perhaps a policy document or a shared drive of vendor contracts — but there is no consistent mechanism for onboarding, no structured assessment workflow, and no central record of who your vendors are or what risks they carry. Conflicts are handled reactively, often only when something goes wrong. Vendor information lives in department-level spreadsheets and email threads, managed by individuals rather than a system. Nothing is searchable. Nothing is auditable.

PROGRAM CHARACTERISTICS:

- No centralized third-party inventory; vendor data is siloed across departments and spreadsheets
- Due diligence is event driven, not systemic. Triggered by audit or incident
- Onboarding timelines are unpredictable, often stretching 60–90 days or longer
- No formal risk triage or scoring; all relationships are treated the same regardless of risk level
- No analytics/reporting capability. No view into third-party ecosystem
- No integration with sanctions databases, adverse media, or any external risk intelligence
- Monitoring is effectively nonexistent: due diligence, when it happens, is a one-time exercise at onboarding
- No visibility beyond the first tier; subcontractor and nth-party relationships are entirely unknown

THE RISK REALITY:

Organizations at this stage are operating blind in all four dimensions of value. No automation means every vendor interaction is manual, slow, and inefficient. Without consistent due diligence, bad decisions get made; vendors are onboarded who should not be, and risks that could have been caught at the gate surface later as incidents. With no centralized inventory, the organization lacks resilience; it cannot even identify which vendors are critical to operations, let alone plan for what happens if one fails. There is no risk intelligence to act on, making it impossible for the organization to move faster or more agilely than its competitors on sourcing, contracting, or market entry because it has no confidence in who it is doing business with consequences.

SIGNS IT IS TIME TO MOVE ON:

- ▶ A compliance audit has flagged the absence of a documented vendor risk process
- ▶ An incident occurred — a data breach, a sanctions violation, a news story about a supplier — that your team had no early warning of
- ▶ The team cannot answer "how many third parties do we have, and which are high risk?" with any confidence



PHASE 2 OF 5

Reactive

"We run assessments when we have to, and hope for the best."

WHAT IT LOOKS LIKE:

The organization has a documented TPRM policy, a dedicated owner, and some basic automation: typically a questionnaire tool or a GRC module. A tiered approach may be nominally in place. But the program remains fundamentally reactive: assessments happen primarily at onboarding, ongoing monitoring is minimal, and the team spends most of its time chasing completions rather than analyzing risk.

PROGRAM CHARACTERISTICS:

- Third-party inventory exists but is incomplete or inconsistently maintained
- Tiered risk classification is applied inconsistently, based on limited data
- Questionnaire-based assessments rely heavily on self-reported vendor information
- Sanctions and watchlist screening active but generates high false-positive rates
- Monitoring is limited to the highest-risk tier; medium and lower-risk vendors are largely unchecked
- No integration between TPRM and other internal compliance processes (COI, G&E, incidents)
- Reporting covers completion rates and open items, not risk distribution or mitigation quality
- Narrow regulatory focus: typically just ABAC and sanctions
- Onboarding timelines remain long (often 30–60 days) creating friction with the business

THE RISK REALITY:

The program creates a false sense of coverage. Analysts spend time on low-risk submissions that should be auto-approved, leaving little capacity for genuine risk analysis. Risk decisions are made on stale data; a vendor whose ownership changes in January has no mechanism to surface that until the next assessment cycle. With monitoring limited to the top tier, there is no early warning when a medium-risk vendor experiences a data breach or sanctions hit. And slow, manual onboarding processes mean compliance creates friction rather than enabling faster business decisions.

HOW TO MOVE FROM PHASE 2 TO PHASE 3:

- ▶ Implement purpose-built TPRM software that provides a centralized, searchable vendor registry as a single source of truth
- ▶ Introduce automated workflow for routing assessments to the right reviewers based on risk level
- ▶ Deploy automated sanctions and adverse media screening with AI-assisted false-positive reduction to reclaim analyst capacity
- ▶ Begin tracking mitigation status, not just questionnaire completion
- ▶ Establish always-on monitoring so that changes to a vendor's risk profile are surfaced as they happen, not at the next assessment cycle



PHASE 3 OF 5

Structured

"We have a process, but it's slow, siloed, and hard to scale."

WHAT IT LOOKS LIKE:

The organization has implemented dedicated TPRM software and documented processes across the vendor lifecycle. Risk triage is more consistent, completion rates have improved, and the team has visibility into assessment status across the portfolio. But the data does not yet connect: TPRM sits in its own system, separate from COI, gifts and entertainment, and incident management. Workflows are rigid, monitoring is concentrated on the highest-risk tier, and sub-tier visibility remains limited.

PROGRAM CHARACTERISTICS:

- Centralized third-party inventory in place with consistent onboarding workflows
- Risk-based tiering applied systematically, with differentiated due diligence by risk level
- Automated questionnaires and workflows reduce manual effort but require IT involvement
- Screening is automated but high false-positive volumes from legacy matching logic
- Real-time monitoring in place for the highest-risk vendors, periodic for medium-risk vendors
- TPRM data is siloed from COI, G&E, incident management, and investigations
- Reporting provides status data but lacks the risk distribution and trend analytics needed to brief leadership
- Supply chain visibility limited to the first tier
- Regional or multilingual gaps create inconsistency in global operations

THE RISK REALITY:

The program looks functional from the outside, but hidden risk persists. A vendor appearing in both a TPRM screening and an employee's COI disclosure is invisible without manual correlation. Concentration risk builds undetected because TPRM data doesn't connect to incident or investigation outcomes. Rigid workflows slow the program's ability to adapt to new regulations or business changes. As monitoring drops off sharply beyond the first tier, the program is only managing the risks it can see.

HOW TO MOVE FROM PHASE 3 TO PHASE 4:

- ▶ Integrate TPRM with COI, G&E, and incident management on a single platform, so every risk signal is visible
- ▶ Deploy AI-powered screening to reduce false positives and expand risk coverage
- ▶ Implement risk-based triage to automatically route low-risk disclosures for auto-approval, freeing reviewers for high-risk cases
- ▶ Build executive dashboards that present risk distribution, trends, and status, not just completion rates
- ▶ Extend monitoring coverage to medium-risk vendors and begin developing a framework for sub-tier visibility



PHASE 4 OF 5

Proactive

"We understand our risk landscape and can demonstrate program effectiveness."

WHAT IT LOOKS LIKE:

TPRM is a continuous, connected, and increasingly intelligent function. Onboarding is faster (under two weeks) as automated screening, AI-powered risk scoring, and configurable workflows eliminate manual bottlenecks. Monitoring covers full vendor portfolio in real time. Connected compliance data means a risk signal is immediately visible in context of that vendor's full risk profile.

PROGRAM CHARACTERISTICS:

- Full third-party lifecycle managed on an integrated platform
- AI-powered screening with precision matching reduces false positives
- Risk-based triage automatically routes low-risk vendors for expedited approval; high-risk vendors trigger enhanced DD
- Continuous monitoring with alerts for adverse media, sanctions, ESG events, and ownership changes
- TPRM connected to compliance ecosystem; vendor risk assessed in full context
- Executive dashboards provide real-time visibility
- Sub-tier visibility expanding: fourth-party/beyond assessed for highest-risk segments
- Supplier concentration risk is identified before disruption hits
- Connected data and real-time monitoring enable incident response in hours, not weeks
- Onboarding up to 50% faster, reducing friction and accelerating time-to-revenue on new supplier relationships

THE RISK REALITY:

The program is stronger, but one opportunity remains: TPRM data is not yet fully a forward-looking strategic intelligence source. Predictive analytics (identifying risk concentration) is the next horizon. The question is no longer "are we covered?" It is "what does the data tell us about where risk is heading?"

HOW TO MOVE FROM PHASE 4 TO PHASE 5:

- ▶ Invest in predictive analytics that identify risk concentration and exposure patterns
- ▶ Extend TPRM due diligence deeper into the supply chain for high-risk segments
- ▶ Establish TPRM program performance as a quarterly KPI reported to the board
- ▶ Integrate into ERM frameworks, ensuring TPRM informs strategic decision-making



PHASE 5 OF 5

Optimized

“Third-party risk is a strategic intelligence source that shapes how we run our business.”

WHAT IT LOOKS LIKE:

TPRM is fully embedded in the organization’s broader risk, ethics, and business strategy. The compliance function uses third-party data alongside regulatory signals, HR data, investigation outcomes, and geopolitical intelligence to build a forward-looking picture of organizational risk. Due diligence is frictionless, vendor assessments are personalized using GenAI, and risk signals are surfaced the moment they emerge across a monitored universe of billions of global data points. The program evolves continuously — driven by data, not just regulatory change.

PROGRAM CHARACTERISTICS:

- TPRM fully integrated into the enterprise risk framework, informing risk scoring across all compliance domains
- Predictive analytics surface emerging risk concentrations by business unit, geography, or supplier network
- AI-generated enhanced due diligence reports delivered in minutes, covering all risk domains
- GenAI personalization delivers role- and region-specific guidance within vendor and employee workflows
- Visibility extends into fourth and fifth-tier relationships, with ownership mapping identifying indirect exposures
- Compliance is a genuine strategic partner; TPRM intelligence informs sourcing, M&A, market entry, and operational decisions
- Board and executive leadership are active program champions; TPRM performance is a quarterly KPI
- Agility is a measurable competitive advantage: faster onboarding, new markets entered with confidence, quicker sourcing decisions
- Resilience is built into operations, disruptions are anticipated

WHAT THIS LOOKS LIKE IN PRACTICE:

At Phase 5, TPRM is not a checkbox. It is an early warning system, a cultural signal, and a competitive advantage. Organizations at this level can demonstrate to regulators, investors, and business partners that their commitment to operating with integrity is operational, built into how the business runs, not bolted on as an annual compliance exercise. They are not asking “did this vendor pass due diligence?” They are ensuring they will know the moment the answer changes.

	 PHASE 1 Informal 1	 PHASE 2 Reactive 2	 PHASE 3 Structured 3	 PHASE 4 Proactive 4	 PHASE 5 Optimized 5
Vendor inventory	None / spreadsheets	Partial, manual	Centralized, siloed	Centralized, integrated	Fully connected, predictive
Due diligence	Ad hoc / none	Questionnaire-based, manual	Tiered, automated	AI-powered, risk-calibrated	Generative AI reports in minutes
Screening	None	Basic sanctions, high false positives	Automated, improving	AI-powered, risk-calibrated	LLM precision matching, full domain coverage
Monitoring	None	Periodic, top-tier only	Ongoing, top-tier only	Continuous, full portfolio	Real-time, predictive, self-updating
Connected risk signals	None	None	Partial	COI + G&E + incidents	Full enterprise risk integration
Sub-tier visibility	None	None	Limited	Expanding	Fourth-party+ systematically assessed
Onboarding speed	60–90+ days	30–60 days	2–4 weeks	Under 2 weeks	Days — AI-accelerated
Analytics	None	Completion rates	Basic reporting	Real-time dashboards	Predictive intelligence
Regulatory readiness	Limited	Low–Moderate	Moderate	High	Full evidence-based
Board reporting	None	Ad hoc	Basic	Regular, structured	Strategic KPI

Informal → Reactive → Structured → Proactive → Optimized

What GAN Integrity Customers Have Achieved



Managing thousands of third parties, Clarios needed a smarter way to handle risk. With GAN Integrity, they built a centralized TPRM program that cut onboarding time by 70%, reduced rework by 20%, and streamlined questionnaires by 37%. The result was an efficient, risk-aligned process that gave compliance full oversight and helped support recognition as one of the world's most ethical companies.

Global Mining Company

Fragmented tools and growing complexity were pulling teams away from where they were needed most. With GAN Integrity, one of the world's largest mining and materials companies unified third-party risk data, embedded risk assessments into global operations, and freed up compliance to focus on the highest priorities. Now, the technology does the heavy lifting — so risk and compliance can focus on high-impact work.

Frequently Asked Questions

We already have a GRC platform that includes TPRM. Is that enough?

Most GRC platforms treat TPRM as a module, not a purpose-built solution. The critical test is connectivity, configurability, and intelligence: Can your platform automatically link a third-party profile to that vendor's relationship with an employee who has filed a COI disclosure? Can it generate an AI-powered due diligence report in minutes when a medium-risk vendor is escalated? Does it triage risk automatically, routing low-risk vendors for auto-approval while flagging anomalies for human review? Can it screen across ESG, data privacy, information security, and sanctions not just ABAC? Purpose-built TPRM functionality goes significantly beyond what most GRC modules offer, and the difference shows up directly in onboarding speed, false-positive rates, and the quality of risk intelligence available to the compliance team.

How long does it typically take to move from one phase to the next?

Organizations that move with intention (clear goals, leadership support, and the right technology partner) typically see measurable progress within one assessment cycle. The most important variable is not time; it is willingness to replace manual processes with purpose-built tools, and to connect TPRM data to the rest of the compliance program rather than managing it in isolation. Moving from Phase 2 to Phase 4 in under a year is achievable with the right platform and commitment.

How do we build the internal business case for investment?

The most effective business cases anchor on three numbers: the cost of the current process, the cost of a compliance failure, and the demonstrable ROI from a more mature program. Research from APAX commissioned in 2023 found that GAN Integrity users report 86% reduced risk exposure, 73% increased employee satisfaction, and 55% observed an increase in ethical behavior — versus significantly lower figures for competitors. GAN Integrity works with customers to build a tailored ROI model that quantifies both the efficiency gains and the risk mitigation value of a more mature program.

What if our completion rates are already acceptable?

Completion rate measures whether a vendor submitted a questionnaire response, not whether the response was accurate, not whether any identified risk was mitigated, and not whether the relationship has changed since submission. Organizations with strong completion rates can still have significant unmanaged exposure. The more important questions are: What percentage of your third-party universe is receiving continuous monitoring, not just periodic reassessment? Are your screening tools generating so many false positives that analysts are missing genuine signals? Can you demonstrate to a regulator today how a specific third-party risk was identified, escalated, and resolved?

What about our fourth-party and sub-tier risk?

This is the industry's fastest-growing blind spot- few organizations assess fourth-party vendors, and even less assess fifth tier and beyond. Yet many of today's most material risks — forced labor, ESG violations, sanctions evasion, and cyber vulnerabilities — frequently originate in indirect tiers. The most advanced TPRM programs are beginning to close this gap using network-level ownership mapping, AI-powered intelligence that can trace beneficial ownership through complex corporate structures, and extended due diligence frameworks that apply differentiated scrutiny to high-risk sub-tier relationships.



Ready to Assess Your Program?

GAN Integrity works with compliance teams at every stage of the maturity curve from organizations building a centralized vendor inventory for the first time, to global enterprises building predictive risk intelligence into their compliance strategy. Our integrated platform unifies TPRM, conflicts of interest, gifts and entertainment, incident management, and policy management in a single connected system, so your compliance team can manage risks in one place and react with agility.

Our team of in-house compliance experts brings both the domain knowledge and the technology to help you move forward with confidence.

To start the conversation, visit ganintegrity.com

References

APAX Partners. GAN Integrity Customer Research. Commissioned by APAX, 2023.

European Commission. *Corporate Sustainability Due Diligence Directive (CSDDD)*. 2024.

German Federal Ministry of Labour and Social Affairs. *Supply Chain Due Diligence Act (Lieferkettensorgfaltspflichtengesetz)*. 2023.

EY. 2023 *Third-Party Risk Management Survey*. Ernst & Young, 2023.

GAN Integrity. *The State of Third-Party Due Diligence 2025: How Compliance Teams Are Managing Scale, Complexity, and the New AI Frontier*. GAN Integrity & Compliance Week, 2025.

Gartner. *Top 3 Strategic Priorities for Chief Compliance and Ethics Officers*. Gartner, 2024.

Gartner. *Third-Party Risk Management Model*. Gartner, 2019.

Rasmussen, Michael. *GRC Market Update: From the Hospital, to Phoenix, Amsterdam, and a Busy European Spring*. GRC 20/20 Research, LLC.

Rasmussen, Michael. *Third Party GRC Maturity Model: A New Paradigm in Governing Third Party Relationships*. GRC 20/20 Research, LLC.

Thomson Reuters. "Adverse Media Screening: An Overview."
legal.thomsonreuters.com/blog/overview-adverse-media-screening

UK Ministry of Justice. *The Bribery Act 2010: Guidance*.
legislation.gov.uk/ukpga/2010/23/contents

US Department of Justice. *Evaluation of Corporate Compliance Programs*. Updated June 2020.
justice.gov/criminal/criminal-fraud/file/937501/download