GAN INTEGRITY

The GAN Integrity Guide to

Conflicts of Interest Program Maturity

Why Your COI Program Maturity Matters

Conflicts of interest are one of the most pervasive — and most underestimated — risks in any organization. They exist in every industry, at every level of seniority, and in every corner of the business. When left unmanaged, they create conditions for fraud, erode internal trust, invite regulatory scrutiny, and cause reputational damage that can take years to recover from. Yet despite the stakes, most organizations still rely on annual email campaigns, spreadsheets, or makeshift tools to manage a risk that is present every day of the year.

The gap between the effort being invested in COI programs and the protection they actually provide has never been more consequential. Regulators are no longer satisfied with evidence of a process existing on paper. The US Department of Justice's guidance for evaluating corporate compliance programs now explicitly asks whether a program is *truly effective* — whether it is understood by employees in practice, whether it adapts as the business evolves, and whether it generates the kind of data that supports real-time decision-making. Boards and executive teams are asking the same questions. A mature COI program is no longer simply a legal safeguard; it is a visible signal of organizational integrity, a competitive advantage in talent and contracting, and an early warning system for broader ethical 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 COI 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 with the infrastructure.

The single biggest accelerant at Phases 1 and 2 is replacing ad hoc processes with purpose-built technology. When disclosures are easy to submit, automatically routed, and centrally stored, completion rates climb — and the compliance team stops spending its time chasing responses and starts spending it on the submissions that actually require judgment.

Extend from once-a-year to always-on.

An annual campaign is a snapshot. Risk happens continuously. Moving to year-round disclosure — where employees can declare a conflict the moment it arises, from any device — closes the nine-month gap that annual campaigns leave open. This single change transforms COI from an administrative exercise into a genuine early warning mechanism.

Connect the data.

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

Use data to predict, not just report.

At the highest levels of maturity, COI programs shift from documenting what happened to anticipating what is likely to happen next. Risk-based triage, targeted campaigns shaped by employee role and geography, and analytics that surface patterns across the organization 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 COI Program Maturity

1 Ad Hoc ····· 2 Reactive ····· 3 Structured ····· 4 Proactive ····· 5 Optimized

PHASE 1 OF 5

Ad Hoc

> *"We have a policy. Somewhere."*

WHAT IT LOOKS LIKE:

The COI process exists on paper — a policy document, perhaps a PDF — but there is no consistent mechanism for employees to disclose, no structured review workflow, and no central record of what has been declared. Conflicts are handled reactively, often only when something goes wrong. Disclosures happen via email or paper forms, managed by individuals rather than a system. Nothing is searchable. Nothing is measurable.

PROGRAM CHARACTERISTICS:

- COI policy exists but has low visibility and limited employee awareness
- Disclosure is event-driven, not systematic — triggered by a complaint or audit finding rather than a process
- All tracking is manual: email threads, spreadsheets, or nothing at all
- No formal review workflow; managers or HR resolve conflicts informally and inconsistently
- Zero analytics or reporting capability
- No integration with onboarding, HR systems, or third-party data
- Scope limited to the most obvious conflict types only

THE RISK REALITY:

Organizations at this stage are flying blind. COI handling is widely recognized as a reflection of broader compliance maturity, and regulators are watching. The DOJ's guidance explicitly asks prosecutors to evaluate whether compliance programs are "truly effective" — and at Phase 1, there is little evidence to show. Reputational damage, missed early warning signals, and audit exposure are the most common and costly consequences.

SIGNS IT IS TIME TO MOVE ON:

- A compliance audit has flagged gaps in COI documentation
- An incident occurred that a functioning disclosure process might have prevented
- The team has no reliable answer to "how many conflicts exist in our organization right now?"

PHASE 2 OF 5

Reactive

> *"We run a campaign once a year and hope for the best."*

WHAT IT LOOKS LIKE:

The organization has a functioning annual disclosure campaign — typically an email-driven questionnaire distributed once a year. Completion rates are tracked, but the definition of "complete" is simply having submitted a response, not having disclosed, managed, or mitigated an actual conflict. The compliance team processes disclosures manually in spreadsheets or a tool not built for COI. There is no year-round mechanism for employees to disclose conflicts as they arise.

PROGRAM CHARACTERISTICS:

- Annual campaign is the primary — often only — disclosure mechanism
- Completion rate is the primary metric, not risk coverage or mitigation quality
- Spreadsheets or email manage the review and resolution process
- No automated triage — every disclosure is reviewed manually regardless of risk level
- Limited or no workflow for manager review, escalation, or mitigation tracking
- Data is siloed and disconnected from third-party risk, investigations, or training
- Scope may cover outside employment and financial interests but remains narrow
- Dependent on one or two individuals to manage the entire process through disclosure season

THE RISK REALITY:

The annual campaign creates a false sense of coverage. An employee who accepts a gift from a vendor in March — nine months before the next campaign — has no structured prompt to disclose. The compliance team spends enormous effort during "disclosure season" manually chasing completions and reviewing low-risk submissions, time that could be spent on genuine risk analysis. Regulators increasingly expect ongoing monitoring, not point-in-time snapshots.

HOW TO MOVE FROM PHASE 2 TO PHASE 3:

- Replace spreadsheets and email with purpose-built COI software that provides a centralized, searchable record of all disclosures
- Introduce automated workflow for routing disclosures to managers and compliance reviewers
- Add an always-on disclosure channel so employees can report conflicts as they arise, not just during the annual campaign
- Begin tracking mitigation status, not just completion

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 moved beyond spreadsheets and implemented dedicated software — but often a point solution not purpose-built for COI, or a broader GRC platform where COI is a module that does not reflect the organization's actual workflows. The compliance team can track disclosure status and generate basic reports, but the system requires significant manual workarounds. Workflows exist but are rigid, making it difficult to handle edge cases, different geographies, or acquisitions. Data lives in the COI tool but does not connect to adjacent compliance processes.

PROGRAM CHARACTERISTICS:

- Dedicated software in place, but COI data disconnected from other compliance processes
- Annual campaign supplemented by some ongoing disclosure capability
- Workflows exist but are limited in configurability — IT involvement often required for changes
- Basic reporting available: completion rates, open items, resolution status
- Manager review is included but may be disconnected or underutilized
- Multilingual capability often limited, creating adoption gaps in non-English-speaking regions
- Completion rates typically 60–75%, but engagement quality is low
- Acquisitions and organizational changes expose gaps in coverage

THE RISK REALITY:

The program looks functional from the outside — there is a system, a process, a report. But hidden risk persists because the data does not connect. A vendor who appears in a third-party risk screening and also in an employee's undisclosed COI declaration is invisible unless someone manually correlates the two datasets. Without connected data, compliance officers cannot identify systemic risk patterns across business units or geographies.

HOW TO MOVE FROM PHASE 3 TO PHASE 4:

- Integrate COI with gifts and entertainment, third-party risk management, and incident management on a single platform
- Deploy targeted campaigns by role, seniority, and geography rather than sending every employee the same questionnaire
- 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 and trends, not just completion status
- Ensure HR system integration keeps manager assignments and org structure current automatically

PHASE 4 OF 5

Proactive

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

WHAT IT LOOKS LIKE:

The organization treats COI as a living risk signal rather than an administrative exercise. Disclosure is year-round, accessible on mobile, and embedded into new hire onboarding. Campaigns are targeted — different employee populations receive different questionnaires based on role, geography, and risk profile. Automated triage routes disclosures by risk level. Real-time dashboards provide continuous visibility into the overall program health.

PROGRAM CHARACTERISTICS:

- Year-round disclosure capability with targeted, risk-based campaigns by role, region, and business unit
- Automated triage: low-risk disclosures auto-approved; high-risk flagged for compliance review
- Connected to gifts and entertainment, third-party risk, investigations, and policy management
- Real-time dashboards tracking disclosure rates, risk distribution, mitigation status, and emerging trends
- Manager review is embedded, tracked, and measured — not optional or ad hoc
- Integration with HR systems keeps employee and org data current automatically
- Multilingual and globally accessible on mobile and desktop
- COI data actively informs training priorities and enterprise risk assessments
- Compliance team can demonstrate program effectiveness to regulators , boards and leadership teams
- Completion rates consistently above 85%

THE RISK REALITY:

The program is materially stronger, but an opportunity remains: conflicts are being managed effectively, but the compliance function is not yet fully leveraging COI data as a forward-looking strategic intelligence source. The question at Phase 4 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 by business unit, geography, or third-party relationship before incidents occur
- Deploy GenAI personalization to deliver role-specific, context-aware compliance guidance
- Extend COI to key third parties and suppliers as part of a your due diligence
- Establish COI program performance as a quarterly KPI reported to the board
- Integrate COI intelligence into enterprise risk management frameworks

PHASE 5 OF 5

Optimized

> *"Conflicts of interest are a strategic intelligence source that shapes our ethics culture."*

WHAT IT LOOKS LIKE:

COI management is fully embedded in the organization's broader risk, ethics, and people strategy. The compliance team uses COI data alongside third-party risk intelligence, regulatory change signals, HR data, and investigation outcomes to build a forward-looking picture of organizational risk. Disclosure is frictionless and culturally normalized — employees understand not just that they must disclose, but why it matters and how it protects them and the organization. Campaigns are personalized at scale using GenAI and HR data to send the right message to the right employee at the right time. The program evolves continuously, reviewed and refined based on what the data reveals.

PROGRAM CHARACTERISTICS:

- COI data fully integrated into the enterprise risk framework and informs risk scoring across compliance domains
- Disclosure rates consistently above 92%, with high-quality submissions and low noise
- GenAI-powered personalization delivers role- and region-specific guidance within employees' daily workflows
- Predictive analytics surface emerging risk areas before incidents are disclosed
- Compliance function is a genuine strategic partner to Finance, HR, Legal, and Procurement
- COI screening extended to key third parties and supply chain partners
- Board and executive leadership are active, measurable champions of the COI program
- COI program performance is a KPI reported quarterly to the board
- Program is continuously reviewed and improved based on data — not just regulatory change

WHAT THIS LOOKS LIKE IN PRACTICE:

At Phase 5, COI 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 employees that their commitment to ethics is operational — built into how the business runs, not bolted on as a compliance exercise.

	PHASE 1 Ad Hoc	PHASE 2 Reactive	PHASE 3 Structured	PHASE 4 Proactive	PHASE 5 Optimized
	1	2	3	4	5
Disclosure mechanism	Ad hoc / paper	Annual campaign	Annual + ongoing	Year-round, targeted	Year-round, AI-personalized
Data management	None / email	Spreadsheets	Dedicated tool, siloed	Integrated platform	Fully connected, predictive
Workflow	Informal	Manual review	Configurable but rigid	Automated triage	Dynamic, self-optimizing
Analytics	None	Completion rates	Basic reporting	Real-time dashboards	Predictive intelligence
Connected risk signals	None	None	Partial	COI + G&E + TPRM + incidents	Full enterprise risk integration
Employee engagement	Low	Moderate	Moderate	High	Culturally embedded
Completion rate	<30%	40–65%	65–80%	85–92%	>92%
Regulatory readiness	Low	Low–Moderate	Moderate	High	Full evidence-based
Board reporting	None	Ad hoc	Basic	Regular, structured	Strategic KPI

Ad Hoc → Reactive → Structured → Proactive → Optimized

What GAN Integrity Customers Have Achieved

These are not projections. They are outcomes delivered by real organizations that committed to moving up the maturity curve.

KONGSBERG

Kongsberg increased COI completion rates from approximately 40% to over 90% in a single year — moving from disconnected manual processes to a centralized platform with automated workflows and enterprise HR integration.

USA Energy Company

A major US energy company reduced disclosure review time from 90 days to under 30 — replacing a home-built system that required manual spread-sheet downloads with automated triage and real-time dashboards that focus time on risk, not data gathering.

Global Payment Services Company

A global payment service company achieved 80% of prior-year disclosures on Day 1 of launch — evidence that when the employee experience is intuitive and the process is frictionless, participation takes care of itself.

Global consulting company research commissioned by APAX in 2023 found that GAN Integrity users report:

86% significantly reduced risk exposure — vs. 50% for competitors

73% increased satisfaction across employees — vs. 40% for competitors

55% observed an increase in ethical behavior — vs. 39% for competitors

Frequently Asked Questions

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

Most GRC platforms treat COI as a module — not a purpose-built solution. The critical test is connectivity and configurability: Can your platform automatically link a COI disclosure to that employee's vendor relationships, gifts received, and any open investigations? Can managers approve on mobile? Does the workflow update automatically when HR data changes? Does it triage risk automatically, or does every submission land in the same queue? Purpose-built COI functionality goes significantly beyond what most GRC modules offer — and the difference shows up directly in completion rates, review time, 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 disclosure cycle. Kongsberg moved from Phase 2 to Phase 4 in under a year. The most important variable is not time; it is willingness to replace manual processes with purpose-built tools, and to connect COI data to the rest of the compliance program rather than managing it in isolation.

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 (team hours during disclosure season, manual review time, IT maintenance of workarounds), the cost of a compliance failure (regulatory fines, legal exposure, reputational damage from an undisclosed conflict that becomes a headline), and the demonstrable ROI from peer organizations. 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 an employee submitted a response — not whether they disclosed an actual conflict, not whether it was reviewed, and not whether any mitigation was put in place. Organizations with 75% completion rates can still have significant undisclosed risk. The more important questions are: What percentage of your workforce is in a role or geography where conflicts are most likely? Are you confident that low-risk disclosures are being triaged automatically and high-risk ones are receiving the scrutiny they deserve? Can you demonstrate to a regulator — today — how a specific conflict was identified, reviewed, and resolved?

GAN INTEGRITY

Ready to Assess Your Program?

GAN Integrity works with compliance teams at every stage of the maturity curve — from organizations moving away from spreadsheets for the first time to global enterprises building predictive risk intelligence into their compliance strategy. 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