GAN INTEGRITY

Developing Third-Party Risk Management Capabilities for a World in Crisis

by Matt Kelly

It is no secret that corporations around the world today struggle to manage their risks. At the center of that struggle are third parties.

In a host of ways, third parties challenge business operations like never before. They can disrupt supply chains stretched around the world; open the door to cybersecurity attacks within your organization; or cause costly compliance failures such as anti-corruption, sanctions, or antitrust violations.

Reliance on third parties is not going to recede any time soon, so businesses will need to tame those third-party risks somehow. Crucial to that goal will be better **incident response capabilities** — first to anticipate all the third-party risks that might arise, and then to have an effective response at the ready when those events do strike.

The good news: most organizations can leverage their prior experience with corporate compliance programs into stronger, more comprehensive third-party risk management programs. Management teams can then turn that better risk management capability into a strategic advantage for years to come.

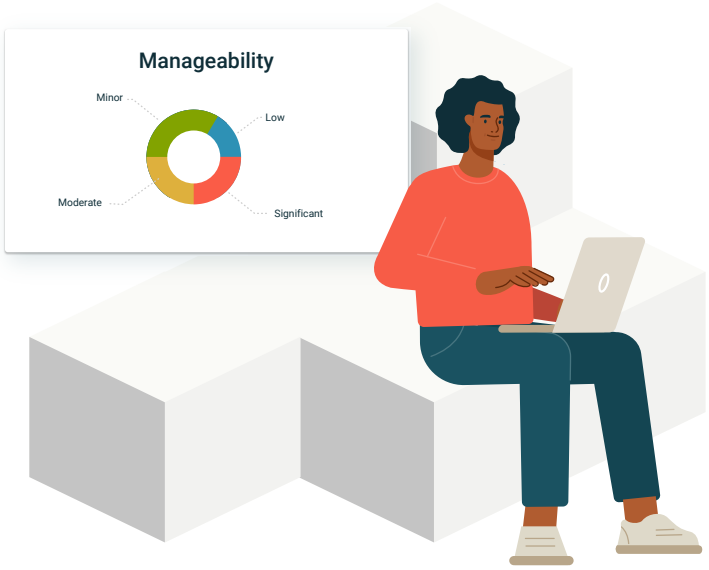
The Changing Nature of Risk

The challenge with third-party risk has several causes.

First, **businesses today use more third parties than ever before**. Even small companies rely on dozens of third parties; large ones might easily use thousands or even tens of thousands.

Second, **businesses use third parties in more ways**, and often in mission-critical ways. For example, a global manufacturing business might use contracted labor at its plants (supply chain risk), overseas agents to drive its international sales (compliance risk), and cloud-based IT services to run R&D, finance, and other functions (cybersecurity risk).

Third, **businesses operate at a scale and manner that leaves their operations "tightly coupled,"** where a failure in one part of the enterprise can disrupt many other parts. With so little room for error, it becomes more important for all parts of the enterprise to run smoothly at all times.



And fourth, **regulators around the world are paying more attention to business conduct**, since governments and the public are more exposed to the consequences of poor conduct. An environmental disaster might ruin the water supply; a cybersecurity failure could leave millions without access to power or bank accounts. Governments are more than ready to enforce tough rules to assure that companies take care to avoid such fiascos.

Bundle all those forces together, and the result is this: a business landscape that is highly complicated and highly interdependent, where even seemingly small failures in one part of your enterprise could have far-reaching consequences elsewhere.

> **"A business landscape that is highly complicated and highly interdependent, where even seemingly small failures in one part of your enterprise could have far-reaching consequences elsewhere."**
>
> *— Matt Kelly*

Hence third-party risk management has become such an urgent priority in the last decade. The risks themselves — supply chain, cybersecurity, compliance, financial — aren't new, **but their severity and unpredictability is**, for all the reasons mentioned above.

In such a world, third-party due diligence is no longer enough for success. Rather, companies must use their due diligence capabilities as the foundation for more comprehensive third-party risk management. Those third-party risk management programs can help you to monitor your overall risk continuously, and then to respond swiftly when one of those risks turns into an adverse event.

That, in turn, allows senior management to make better decisions about achieving business objectives, without worrying that an errant third party might derail your plans.

New Pillars of Risk Management and Response

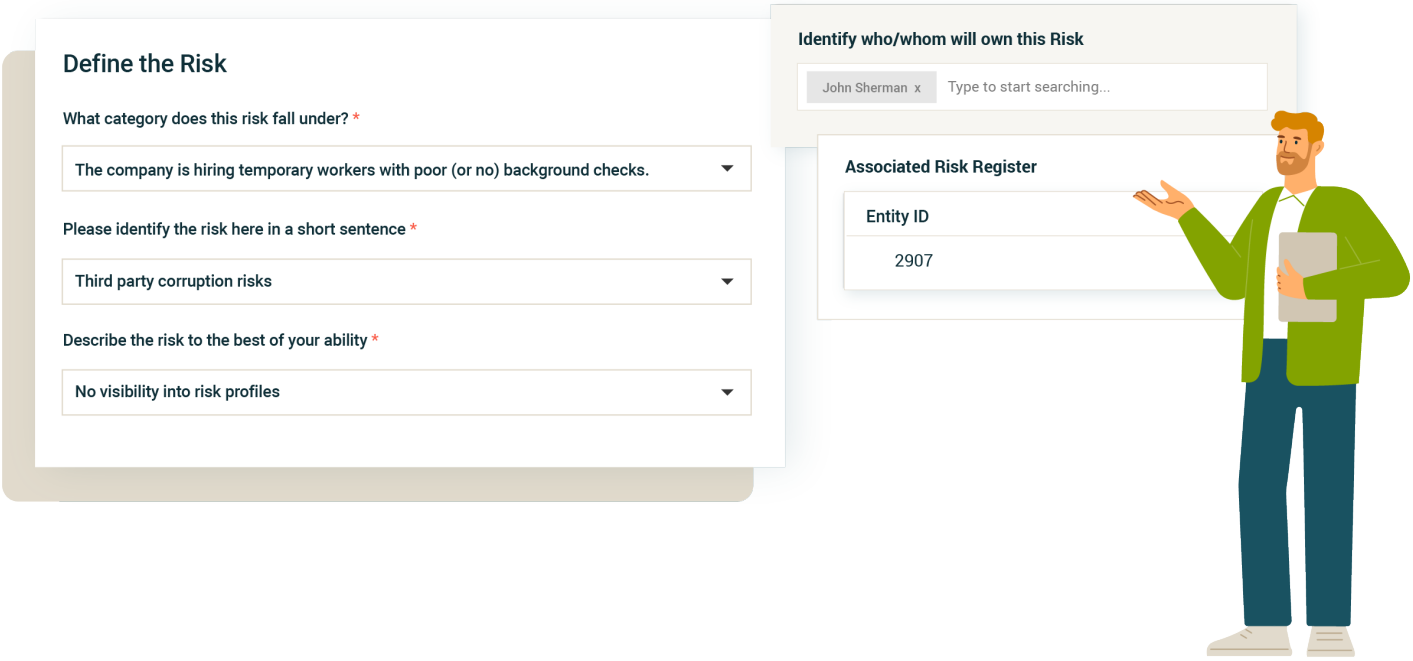
To achieve strong third-party risk management, a business must be able to do four fundamental tasks:

- Identify risks facing the business;
- Implement controls to keep those risks at suitable levels;
- Monitor the risks to determine when they rise to dangerous levels;
- Respond with appropriate steps when a risk does come to pass.

Working backwards from those four tasks, companies can reverse-engineer the capabilities they'll need to get those tasks done.

The first capability is risk assessment, so the organization can identify and understand all the third-party risks it faces. Most likely, you'll need to assemble an in-house risk committee from across the enterprise, to discuss how the business uses and depends on third parties and what might happen if those relationships falter. For example, the risk committee might be led by a company's chief risk officer or head of internal audit, with representatives from legal, compliance, procurement, IT security, sales, and other important business functions.

Second is an ability to implement policies, procedures, and other controls, to keep the risks you've identified at acceptable levels. This might entail policy management tools, to assure that management develops one set of policies that communicate uniform messages across the enterprise. It might also include contract management, to assure that you can enforce standards of conduct, cybersecurity, delivery, and other matters to all your third parties as necessary. Training, internal reporting hotlines, and due diligence procedures would all be important tools too.



Third is an ability to monitor how third parties interact with your enterprise and behave overall. Monitoring is seldom easy. Risk managers will need to track data across multiple business functions, and weave them into a cohesive larger picture that connects back to your risk assessment. For example:

- The IT security team would need to monitor interactions with cloud-based technology vendors, and issues with mission-critical vendors would need priority escalation;
- The compliance team would need to monitor adverse media reports, lawsuits, and other indicators of compliance risks among third parties;
- The procurement or operations team would need to monitor delivery schedules and pricing for supplies, again with mission-critical suppliers getting priority escalation.

Many monitoring tasks can be automated with proper workflow technology. That technology will still need to incorporate escalation triggers tied to your organization's top risks, so that the right managers within your business can respond in a timely fashion when something goes wrong.

To that point, **companies will also need an ability to execute response plans when a risk turns into an adverse event**. This requires risk management teams to do some work in advance, such as analyzing their third party population for critical vendors or conducting table-top exercises to understand how various events (say, a cybersecurity breach) might disrupt operations. Compliance, legal, and security teams should then draft response plans; and those plans should include specific details such as which executives perform what tasks, in what order.

The goals in building a third-party risk management program are always transparency, agility, and responsiveness. Management teams need a clear understanding of the risks their third-party relationships pose, plus an ability to respond quickly (and effectively) when those relationships somehow go awry.

Leveraging Compliance Experience for Supply Chain Expertise

The foundation of third-party risk management is the ability to understand who your third parties are and what risks they pose. Due diligence is an invaluable part of that effort — and moreover, it's something that compliance teams have been doing for years. So the need for third-party risk management is an excellent opportunity for compliance teams; they can play crucial roles in getting the program started and providing ongoing help.

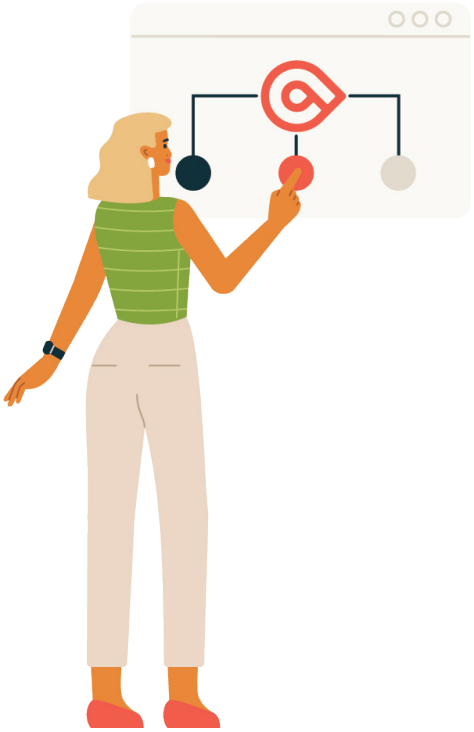
Where compliance officers are already experienced, and can contribute the most:

- Third-party onboarding and due diligence;
- Remediation of weak controls, such as poor policies and procedures;
- Disclosure of privacy breaches or violations of law to regulators;
- Reporting to the board or senior management.

That said, other elements of third-party risk management are typically not a compliance officer's strong suit. Among them:

- Scenario planning, especially for supply chain or cybersecurity disruptions;
- Monitoring the performance of IT vendors and suppliers;
- Drafting business continuity plans;
- Running table-top exercises to assess operational disruption.

This raises an important question: Who should run a third-party risk management program? Compliance officers can help with risk assessment, due diligence, policy management, remediation, and other issues; but third-party risk management goes *beyond* traditional compliance. It also considers operational risks and develops plans to modify operations based on risks that happen. So a chief operating officer, chief risk officer, or chief information security officer might be the better candidate to run third-party risk management, with close assistance from the compliance team.



Each organization will need to answer that question for itself, depending on its structure, business, and management team. Still, all organizations will also need to consider two other points to assure that they can "bridge the gap" from regulatory compliance to true third-party risk management.

First, do you have the right technology for monitoring, reporting, and escalation? Without an ability to monitor how your third parties are behaving, and without the right information flowing to the risk management team, your business can't implement response plans as necessary.

Second, are all risk oversight functions (compliance, legal, IT security, internal audit, and more) aligned on what the company's biggest risks are? If your internal team isn't in agreement about the organization's most pressing risks, and how third parties contribute to them, you won't be able to implement mitigation steps in an effective, efficient way.

Conclusion

Third-party risk management will be essential for corporate success in years to come. The question is whether organizations will **react** to third-party risks in a piecemeal fashion as adverse events happen; or **manage** third-party risks in a more holistic way, with deft and efficient incident response.

A strong compliance program will always be the foundation for third-party risk management — but businesses will need more, too. They'll need technology that can help with scenario-planning, data analytics, and reporting. They'll also need strong partnerships across the enterprise to be clear on the role that third parties should play in your operations, which risks are top priority, and who will take what actions when a third-party risk goes wrong.

Compliance officers can play important roles in leveraging your experience with third parties into that risk management capability organizations will need in the future; in a roundabout way, today's increasingly risky world is an excellent career opportunity.

Seizing that opportunity will require leadership, focus, and technology. The payoff, however, will echo from the boardroom to the corporate hallways to the bottom line.

GAN Integrity enables the world's largest brands to do the right thing.

We fulfil our mission by enabling global teams to manage ethics, compliance, and risk with our Integrity Platform, a no-code application building platform.

Seadrill DANONE NORTH AMERICA CLARIOS BARRICK infront

Schedule a meeting to start driving ethical change

To contact us, visit **ganintegrity.com**