STRATEGIC PERSPECTIVES

THE EVOLUTION OF THIRD-PARTY DUE DILIGENCE

AUGUST 2026

The Evolution of Third-party Due Diligence

Executive Summary

The recent designation of Primeiro Comando da Capital (PCC) and Comando Vermelho as Foreign Terrorist Organizations (FTOs) by the United States has renewed the discussion around third-party risk management. However, the significance of that debate extends well beyond the legal implications of the designation itself. It raises a broader question: whether traditional third-party due diligence processes remain sufficient to identify and understand the risks that may arise through customers, suppliers, intermediaries, and other third parties with whom organizations conduct business.

This question is particularly relevant for companies operating in jurisdictions such as Brazil and Bolivia, where various reports have identified the presence or activities of organizations designated as FTOs, underscoring the need for a broader and more dynamic approach to third-party risk assessment.

A Shift in Expectations

Traditional third-party due diligence remains an essential component of any compliance program, but expectations regarding its scope have evolved. It is no longer enough to demonstrate that an organization has established third-party due diligence procedures or completed documentary reviews. Increasingly, organizations are expected to show that the level of diligence applied was proportionate to the risks involved and that the information obtained provided a reasonable basis for the decisions ultimately made.

The Limits of Traditional Third-party Due Diligence

Corporate records, public registries, beneficial ownership information, and sanctions and watchlist screening remain the starting point of any meaningful third-party assessment. However, these tools do not always provide a complete picture of the risks associated with a business relationship. The challenge today is no longer simply to collect more information, but to determine when the information available is sufficient to reasonably understand the level of risk an organization is prepared to accept.

The Challenge for Companies Operating in Bolivia

Leading international third-party due diligence frameworks establish common objectives while deliberately avoiding a single prescribed methodology. For companies operating in Bolivia, this means adapting their third-party due diligence processes to local conditions without lowering the expected standard of care. The effectiveness of a methodology does not depend on replicating procedures used in other jurisdictions, but on its ability to

generate relevant and reliable information that allows organizations to properly assess the risks associated with each business relationship.

From Assessment to Decision-Making

The most significant evolution lies not in requiring more controls, but in better understanding the purpose of third-party due diligence. Third-party due diligence is not intended to eliminate the possibility of making an incorrect decision. Rather, its purpose is to provide a reasonable basis for making informed decisions that are proportionate to the risks involved and capable of withstanding subsequent scrutiny. From this perspective, third-party risk management evolves from a purely compliance function into a broader tool of corporate governance and business decision-making.

Five Questions that Deserve a Fresh Look

The developments described in this article invite organizations to reconsider five fundamental aspects of third-party risk management:

- **What information would actually change our decision?** The quality of a third-party due diligence review depends not on the volume of information collected, but on identifying the information that could meaningfully influence the decision to enter into or maintain a business relationship.
- **When is the standard third-party due diligence process no longer sufficient?** Standardized procedures promote consistency, but they are not always appropriate for transactions involving elevated or atypical risks. The critical question is knowing when the assessment methodology should be adapted.
- **Who should decide whether to accept a particular risk?** Third-party due diligence informs business decisions but does not replace them. Organizations should clearly define who has authority to accept different levels of risk, under what criteria, and through what documentation and escalation procedures.
- **Would we be able to explain this decision five years from now?** Proper documentation involves more than retaining the information reviewed during the assessment. It also requires preserving the reasoning that supported the decision so it can be explained and defended during audits, investigations, or other future reviews.
- **What developments should trigger a reassessment of a third party?** Approving a third-party should not be viewed as a final decision. Effective third-party risk management requires identifying the events or changes that could materially alter the risk profile of a business relationship and warrant a renewed assessment.

Ultimately, the value of third-party due diligence no longer lies in the amount of information it collects, but in its ability to provide organizations with a reasonable basis for making decisions that can be explained and defended when necessary.

Introduction

For years, companies have invested significant resources in strengthening their compliance programs. Internal policies, third-party due diligence procedures, beneficial ownership verification, and anti-money laundering controls have become standard components of corporate governance and risk management. Yet recent developments across the region suggest that a fundamental question remains increasingly relevant: do the mechanisms companies use to assess their counterparties enable them to adequately understand the risks associated with those relationships?

The recent designation of Primeiro Comando da Capital (PCC) and Comando Vermelho as Foreign Terrorist Organizations (FTOs) by the United States has sparked considerable discussion among businesses, financial institutions, and legal advisors across Latin America. Beyond the specific implications of that designation, the debate has highlighted a broader concern: the growing difficulty of identifying risks that arise not within an organization's own operations, but through its customers, suppliers, intermediaries, business partners, and other third parties with whom it interacts on a daily basis.

The significance of this discussion lies not only in the legal consequences of a particular designation, but also in the broader question it raises for organizations operating in increasingly complex risk environments. Are traditional third-party due diligence processes still sufficient to identify and assess risks whose complexity may extend beyond the information available in public records and other conventional documentary sources?

This question extends well beyond any single jurisdiction or industry. It reflects a broader shift in expectations regarding what it means to truly know a business counterparty. Reviewing corporate records, public registries, and other formal sources of information remains an essential part of any third-party due diligence process. Increasingly, however, organizations are being asked to consider whether those measures alone provide a sufficiently robust understanding of the risks that may arise from a commercial relationship.

The evolution of these expectations does not diminish the value of traditional third-party due diligence. Rather, it underscores the need to view third-party due diligence not simply as an exercise in information gathering, but as a risk-based process designed to support informed business decisions. As third-party risk becomes more complex and interconnected, the central challenge is no longer whether organizations have third-party due diligence procedures in place, but whether those procedures generate the information necessary to make decisions that are proportionate to the risks involved and capable of withstanding future scrutiny.

1. A Shift in Expectations, Not Just in the Rules

Over the past several years, third-party risk management has undergone a significant transformation. Identifying customers, suppliers, intermediaries, and business partners; verifying beneficial ownership; and reviewing public records and sanctions lists remain fundamental elements of any effective compliance program. Increasingly, however, the global compliance conversation has shifted toward a different question: it is no longer enough to demonstrate that an organization has implemented third-party due diligence procedures. Organizations are now expected to show that those procedures are appropriate for the risks their business faces.

This shift does not suggest that traditional third-party due diligence has lost its value, nor does it mean that every organization should adopt increasingly burdensome controls. Rather, it reinforces one of the core principles of modern compliance programs: risk management should be proportionate to risk.

Leading international frameworks no longer focus solely on whether an organization has formal policies and procedures in place. They also examine whether those procedures have been designed with the organization's specific risk profile in mind, whether the information gathered provides a reasonable basis for decision-making, and whether the third-party due diligence process evolves as business circumstances and risk factors change. In other words, the emphasis is shifting from the mere existence of controls to the effectiveness and reasonableness of their application.

The discussions prompted by the recent designation of Primeiro Comando da Capital (PCC) and Comando Vermelho as Foreign Terrorist Organizations by the United States illustrate this evolution. Although the debate began with a specific regulatory measure, it quickly expanded beyond its immediate legal consequences. The broader question became whether traditional third-party due diligence processes are capable of identifying risks that may arise through seemingly legitimate corporate structures or commercial relationships that, based solely on documentary review, present no obvious warning signs. Put differently, the debate highlighted the need to reconsider whether conventional third-party due diligence remains sufficient in an increasingly complex and interconnected risk environment.

This shift in perspective also changes the way third-party due diligence itself should be understood. For many years, the emphasis was on demonstrating that specific verification steps had been completed: identifying the counterparty, reviewing its corporate records, determining its beneficial owners, and consulting publicly available sources of information. Those steps remain essential, but they are no longer the end of the analysis. Increasingly, organizations are expected to explain why a particular level of review was considered appropriate, how the third party's risk profile was assessed, and why the information obtained was sufficient to support the decision to establish or continue the business relationship.

The distinction may appear subtle, but it reflects a meaningful evolution in the way organizations manage risk. The focus is no longer simply on complying with a prescribed process; it is on demonstrating that the process was capable of producing a reasonable and informed assessment of the risks involved. That evolution also challenges a long-standing assumption: that the information traditionally obtained through third-party due diligence will always be sufficient to understand the risks associated with a business relationship.

2. The Risks that Do Not Always Appear in Public Records

For decades, third-party due diligence has been one of the primary tools organizations use to manage the risks associated with customers, suppliers, business partners, and other third parties. Reviewing corporate records, identifying beneficial owners, conducting public record searches, and screening against sanctions and watchlists remain essential steps in understanding with whom an organization is doing business.

Yet the growing focus on risks associated with transnational criminal organizations has exposed a limitation that often receives less attention: the information available through public records and other documentary sources may not provide a complete picture of the risks associated with a business relationship.

This limitation is not the result of any deficiency in traditional third-party due diligence. On the contrary, these processes were designed to identify objective and verifiable information about a third party. The challenge arises when certain risks are not readily reflected in corporate records, public registries, or the other sources typically relied upon during a third-party due diligence review.

Recent designations of transnational criminal organizations have not diminished the value of traditional third-party due diligence. Rather, they have underscored a different reality: some of the risks that concern organizations today simply cannot be identified through documentary review alone.

As a result, the discussion has increasingly shifted from verifying information to developing a broader understanding of the context in which a third-partyoperates. Factors such as the nature of commercial relationships, the consistency between a company's stated activities and its actual operations, the use of intermediaries, exposure to particular markets or sectors, and potential reputational concerns have become increasingly relevant to third-party risk assessments.

This evolution is particularly evident in the discussions that have followed the recent designation of criminal organizations in the region. One of the principal concerns raised by compliance professionals and corporate investigations practitioners has not been limited to new regulatory restrictions or legal risks. Rather, it has focused on whether

organizations are equipped to identify connections, relationships, or circumstances that may not be apparent from the traditional sources used in third-party due diligence.

As expectations from regulators, financial institutions, investors, and business partners continue to rise, organizations face increasing pressure to demonstrate not only that they have formally assessed their third parties, but that they have developed a reasonable understanding of the risks those relationships may present.

The absence of red flags in public records or other documentary sources should not automatically be equated with the absence of risk. Increasingly, organizations are re-evaluating how they assess third parties in light of this reality. For companies operating in markets such as Bolivia, where access to certain sources of information may be more limited than in other jurisdictions, this evolution presents an additional challenge: how to design third-party due diligence processes that meet international expectations while remaining practical and effective within the local operating environment.

3. What Does This Mean for Companies Operating in Bolivia?

Responding to these evolving expectations does not require organizations to replicate third-party due diligence methodologies developed for other jurisdictions. Rather, it requires a clear understanding of the purpose of third-party due diligence and how that objective can be achieved within the context in which the organization operates. The challenge is not to adopt identical procedures, but to meet the same standard of care through processes that are appropriate for the local environment.

Leading international third-party due diligence frameworks share a common principle: the scope and depth of a review should be proportionate to the risks presented by a particular business relationship. At the same time, they deliberately avoid prescribing a single methodology for achieving that objective. This flexibility reflects a practical reality: the availability of information, market structures, and business practices vary considerably across jurisdictions.

Adapting a third-party due diligence methodology should not be understood as lowering the standard of care. Rather, it recognizes that achieving the same objective may require different tools depending on the jurisdiction and the circumstances of the engagement. Accordingly, the effectiveness of a third-party due diligence process should not be measured by the number of verification steps it includes, but by its ability to generate relevant, reliable, and sufficiently robust information to support an informed assessment of the risks associated with a particular business relationship.

This distinction is readily illustrated by routine commercial transactions. A company onboarding a new distributor, strategic supplier, or commercial intermediary in Bolivia will generally be able to verify the third party's legal existence, corporate authority, and other basic corporate information through available public sources. Depending on the risk

profile of the engagement, however, those checks may not be sufficient to answer the questions that ultimately determine whether the relationship presents an acceptable level of risk. The key issue is therefore not how many documents have been reviewed, but whether the third-party due diligence process has generated enough meaningful information to enable the organization to understand the risks that the relationship presents.

This is perhaps one of the principal lessons emerging from the regional debate following the designation of PCC and Comando Vermelho as Foreign Terrorist Organizations. The discussion has reinforced that the effectiveness of a third-party due diligence methodology does not depend on an ever-expanding list of verification procedures. Rather, it depends on the methodology's ability to produce the information necessary to understand the risks of a business relationship within the context in which the organization operates.

For companies operating in Bolivia, this represents both a challenge and an opportunity. The challenge lies in navigating an environment where certain sources of information may be less accessible than in more mature markets. The opportunity lies in designing risk-based third-party due diligence processes that reflect local realities while remaining aligned with internationally recognized compliance standards. Ultimately, organizations that can demonstrate a thoughtful, proportionate, and well-documented approach to third-party risk assessment will be better positioned to meet the expectations of regulators, financial institutions, investors, and business partners alike.

4. When Third-party Risk Management Becomes More Than a Compliance Function

The evolution described thus far has practical implications that extend well beyond regulatory compliance. If third-party due diligence is no longer limited to verifying information but instead seeks to develop a reasonable understanding of the risks associated with a business relationship, responsibility for managing those risks can no longer rest exclusively with the Compliance function.

Decisions to engage a strategic supplier, appoint a distributor, retain an intermediary, or enter into a commercial partnership are fundamentally business decisions. However, when those relationships give rise to significant legal, financial, or reputational risks, they cease to be purely commercial. Nor are they exclusively legal decisions. Rather, they are business decisions that require organizations to balance commercial objectives with a well-informed assessment of risk.

This reflects one of the most significant developments in third-party risk management. For many years, third-party due diligence was viewed primarily as a prerequisite for approving a business relationship. While that remains true, it no longer captures the full purpose of the process. Third-party due diligence is not intended to eliminate the possibility that an

organization may make an incorrect decision. Instead, its purpose is to provide a structured, informed, and proportionate basis for decision-making. From this perspective, the information generated during a third-party due diligence review is no longer an end in itself; it becomes the foundation upon which an organization determines whether a particular business relationship is consistent with its risk appetite.

This shift also has important implications for internal governance. Increasingly, the challenge is not determining whether a third-partyhas satisfied a prescribed list of documentary requirements. Rather, it arises when the available information identifies potential risks without providing definitive answers. In those circumstances, the critical questions become: Who has the authority to decide whether those risks are acceptable? What criteria should guide that decision? How should the decision be documented and, where appropriate, escalated?

In practice, these situations are far from exceptional. An organization may need to engage a new supplier or intermediary quickly in order to pursue a commercial opportunity, while the third-party due diligence process reveals circumstances that warrant further scrutiny without necessarily precluding the relationship. Balancing commercial imperatives with effective risk management has become one of the defining challenges of modern compliance programs.

The discussions following the designation of PCC and Comando Vermelho illustrate this evolution. Rather than demonstrating the need for ever more extensive controls, they highlight a different reality: even well-designed third-party due diligence processes may produce situations in which the available information does not lead to clear-cut conclusions. In those cases, the central issue is not whether the third-party due diligence process was completed, but whether the organization can demonstrate that it followed a reasonable and well-governed process for reaching and supporting its decision.

Viewed through this lens, third-party due diligence becomes more than a tool for regulatory compliance. It is an essential element of corporate governance, enabling organizations to allocate decision-making authority, define who may accept particular levels of risk, establish objective escalation criteria, and ensure that business decisions are supported by a consistent and proportionate assessment of risk.

Ultimately, the effectiveness of a third-party due diligence program should not be measured solely by the number of controls it contains or the volume of information it collects. Its true value lies in providing organizations with a decision-making framework that enables them to make informed, risk-based decisions that can withstand scrutiny from regulators, investors, counterparties, and other stakeholders.

5. Five Questions Every Organization Should Be Asking About Third Party Risk

The developments discussed throughout this article have an important practical implication: the effectiveness of third-party due diligence no longer depends solely on the existence of policies, procedures, or controls. Increasingly, it depends on the quality of the decisions an organization is able to make when information is incomplete, risk cannot be eliminated entirely, and commercial considerations require action.

In this context, strengthening third-party due diligence does not necessarily mean introducing additional controls. More often, it requires organizations to reconsider how key decisions are made and whether the criteria used to support those decisions remain appropriate in light of increasingly complex risk environments.

Against that backdrop, there are five questions that deserve renewed attention.

1) What Information Would Actually Change Our Decision?

One of the most common responses to a complex transaction is to request additional information. Experience shows, however, that collecting more documents does not necessarily reduce uncertainty or improve decision-making. Beyond a certain point, organizations may spend additional time gathering information and building increasingly comprehensive files without materially improving their understanding of the risks associated with a business relationship.

Consider a company seeking to appoint a new distributor in a market where it has not previously operated. It may be able to verify the distributor's legal existence, identify its directors and beneficial owners, and review other relevant corporate information. Yet those checks may not answer the question that ultimately matters: is there a reasonable basis to conclude that this third-party will conduct business in a manner consistent with the organization's legal, ethical, and compliance expectations?

The more useful question, therefore, is not what additional information can be obtained, but what information would genuinely influence the organization's decision. This distinction helps separate information that is merely available from information that is genuinely decision-relevant, preventing third-party due diligence from becoming an exercise in document collection rather than risk assessment.

Organizations with the most effective third-party due diligence programs typically define in advance the information that is material for different types of transactions, counterparties, and risk profiles. As a result, the depth of the review is driven by risk rather than by the volume of documentation available.

Ultimately, the quality of a third-party due diligence review is measured not by the amount of information collected, but by its ability to generate the information that is most relevant to an informed decision.

2) When is the Standard Process No Longer Enough?

Standardized third-party due diligence procedures serve an essential purpose. They promote consistency, reduce unnecessary discretion, and allow organizations to assess large numbers of third parties efficiently. By their nature, however, standardized procedures are designed for ordinary situations and may not always be appropriate for higher-risk or atypical transactions.

Consider a company engaging an intermediary to support negotiations in a jurisdiction where it has never operated before. Applying exactly the same third-party due diligence process used to onboard a low-risk supplier may be procedurally correct while still being inadequate to understand the risks associated with that engagement.

The key question is therefore no longer whether the prescribed procedure was followed, but whether it was the right procedure for the risks presented by the relationship. That distinction often separates compliance programs that simply follow established processes from those that effectively support risk management.

Organizations that manage third-party risk most effectively do more than establish standardized procedures. They also define the circumstances in which additional review, enhanced third-party due diligence, or alternative assessment methods are warranted. The true strength of a third-party due diligence framework is rarely tested in routine transactions; it is tested when judgment is required.

3) Who Should Decide Whether a Risk Is Acceptable?

Every third-party due diligence review ultimately reaches the point where a business decision must be made. That moment marks the transition from technical assessment to business judgment.

Imagine a commercial opportunity that must be pursued quickly. The third-party due diligence review identifies factors that justify further inquiry, but none that clearly preclude proceeding. The business team believes that delaying the transaction could jeopardize an important opportunity. Compliance recommends additional review. Legal concludes that there is no legal impediment to moving forward.

In situations such as these, the central question is rarely whether risk exists. Rather, it is who within the organization should determine whether that risk is acceptable.

Organizations that manage these situations effectively generally establish clear governance frameworks defining decision-making authority, identifying which risks require additional review or escalation, and specifying the circumstances under which particular risks may be accepted. Such frameworks do not replace professional judgment; they provide a structured process within which that judgment can be exercised.

After all, the purpose of third-party due diligence is not to replace business judgment, but to ensure that business decisions are made on a reasonable, informed, and risk-based basis.

4) Would We Be Able to Explain This Decision Five Years from Now?

Well-documented decisions preserve more than evidence -- they preserve the reasoning that supported them.

Years after entering into a business relationship, an organization may be required to explain its decision to regulators, auditors, financial institutions, investors, law enforcement authorities, or even a new management team that had no involvement in the original assessment. In those circumstances, retaining the documents reviewed during third-party due diligence is important, but it is rarely sufficient.

The more significant question is often: why, based on the information available at the time, was it reasonable to proceed?

Proper documentation therefore involves more than maintaining files or preserving reports. It requires recording the context in which the decision was made, the risks that were identified, the factors considered most significant, and the rationale supporting the conclusion that the relationship was consistent with the organization's risk appetite.

Over time, the ability to explain why a decision was reasonable often becomes a stronger indicator of the maturity of a compliance program than the volume of documentation contained in the file. Organizations rarely face criticism because they failed to retain one additional document; more frequently, they struggle to reconstruct the reasoning that supported a decision years earlier.

5) What Should Trigger a New Assesment?

There is a natural tendency to view third-party due diligence as complete once a third-party has been approved. In reality, every approval is based on assumptions: who owns or controls the company, how it conducts its business, the markets in which it operates, and the role it plays in the transaction.

Those assumptions may change long before the law changes or before any obvious compliance issue emerges.

Consider a third-partythat was assessed two years ago. Since then, it has acquired new shareholders, expanded into different markets, or materially changed its role within the supply chain. None of those developments necessarily requires terminating the relationship. They do, however, warrant reconsidering whether the assumptions that originally supported the decision remain valid.

For this reason, organizations that view third-party risk management as an ongoing process generally complement periodic reviews with clear criteria for identifying events that could materially alter a third party's risk profile. Monitoring therefore becomes driven not only by the passage of time, but by changes in risk.

No business decision remains appropriate indefinitely. It remains appropriate only so long as the assumptions on which it was based continue to hold true. Effective third-party due diligence does not end when a third-party is approved; it requires organizations to revisit whether the reasons that justified that decision remain valid as risks evolve.

Conclusion

The evolution of third-party due diligence reflects a broader shift in the way organizations are expected to manage risk. The question is no longer whether a company has implemented third-party due diligence procedures, but whether those procedures provide a reasonable basis for understanding the risks associated with a business relationship and for supporting the decisions ultimately made.

This evolution does not require organizations to pursue ever more extensive investigations or to eliminate all uncertainty. Rather, it calls for a risk-based approach that is proportionate to the circumstances, informed by reliable and relevant information, and capable of adapting as risks evolve.

For companies operating in jurisdictions such as Bolivia, this means designing third-party due diligence processes that reflect local realities while remaining consistent with internationally recognized standards. The effectiveness of those processes should not be measured by the number of documents collected or the volume of checks performed, but by their ability to generate meaningful information that supports sound business judgment.

Ultimately, the true value of third-party due diligence lies not in preventing every adverse outcome, but in enabling organizations to make informed, well-reasoned, and defensible decisions. In an increasingly complex regulatory and risk environment, that is becoming one of the defining characteristics of an effective compliance program.

About PPO Indacochea

PPO Indacochea is Bolivia's largest law firm, with leading practices across all areas of law. Clients know they can rely on PPO Indacochea for their most challenging legal and business matters. PPO Indacochea's 80 attorneys and more than 180 professionals work diligently to provide exceptional service, sophisticated advice, and creative, practical solutions.

PPO Indacochea is the law firm with the widest geographic coverage in Bolivia, with offices in five cities: La Paz, Cochabamba, Santa Cruz, Sucre, and Cobija.

Authors

Andrea Lizárraga
Senior Associate
alizarraga@ppolegal.com

Lindsay Sykes
Partner
lsykes@ppolegal.com

Fernanda Ribera
Senior Associate
fribera@ppolegal.com

Offices

Santa Cruz

- Av. San Martín
  Edif. Manzana 40
  Torre 2 | Piso 27

- Av. Piraí N° 2115
  Esq. Baracea

La Paz
Av. Ballivián 555
Edif. El Dorial,
Piso 14

Cochabamba
Calle Papa Paulo N°604
Edificio Empresarial Torre 42
Piso 6

Sucre
Calle Ayacucho Nº255
Piso 2

Cobija
Avenida 16 de Julio
N°149
Centro

Phone
(+591) 620 02 020