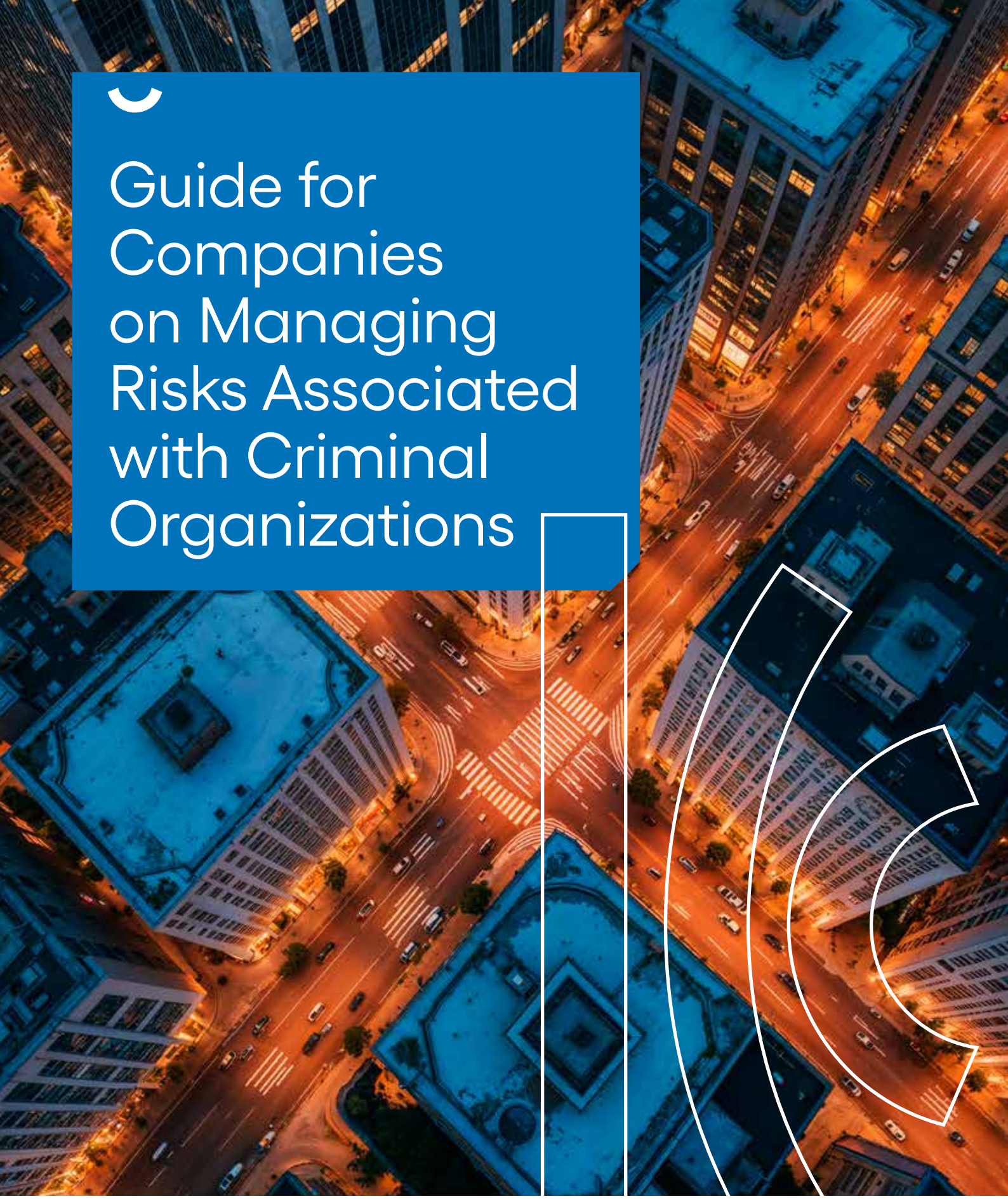
Guide for Companies on Managing Risks Associated with Criminal Organizations



Prepared by ICC Brasil

In Collaboration with the Brazilian Office of the Comptroller General (CGU)

ICC Brasil

CONTROLADORIA-GERAL DA UNIÃO

GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO

Guide for Companies on Managing Risks Associated with Criminal Organizations

ICC Brasil, with the collaboration of the Brazilian
Office of the Comptroller General (CGU)
April 2026

Table of Contents

Foreword **6**

1. Introduction **7**

2. Context, Diagnosis, and Nature of Risks **8**

3. Governance Proposals for Risk Management **14**

3.1. Proposals for the Governance and Compliance Process 14

3.2. Minimum Policies and Procedures 18

3.3. Risk Management Proposals 20

3.4. Proposals for Third-Party Due Diligence 22

3.5. Proposals for Monitoring Mechanisms 28

3.6. Proposals for Training and Organizational Culture 32

4. Proposals for Incident Management and Decision-Making **34**

4.1. Proposals for Information Identification, Recording, and Preservation 34

4.2. Proposals for Internal Assessment and Escalation 36

4.3. Proposals for Internal Reporting Channels 39

4.4. Proposals for Reporting to Competent Authorities 40

4.5. Proposals for Protection Measures, Business Continuity, and Crisis Management 42

5. Final Proposals **44**

Checklist **46**

Definitions

This Guide was developed based on standards such as:

- Law No. 12.846/2013 (Anti-Corruption Law), and its Regulatory Decree No. 11.129/2022;
- Law No. 9.613/1998 (Money Laundering and Terrorist Financing Law);
- Law No. 13.260/2016, Law No. 13.709/2018 (General Data Protection Law);
- Law No. 12.850/2013 (Criminal Organizations Law);
- Law No. 9.296/1996 (Interception Law);
- COAF Resolution No. 36/2021;
- BACEN Circular Letter No. 4.001/2020;
- BACEN Circular No. 3.978/2020;
- BACEN Resolution No. 150/2021;
- BACEN Normative Instruction No. 262/2022;
- BACEN Resolution No. 44/2020;
- AML/CFT Communication No. 43.419/2025;
- Law No. 13.810/2019 (United Nations Security Council Sanctions);
- Decree No. 9.825/2019;
- SUSEP Circular No. 612/2020;
- CNSP Resolution No. 393/2020;
- CVM Resolution No. 50/2021;
- CMN Resolution No. 4.968/2021,
- Previc Instruction No. 34/2020; and
- Decree No. 10.270/2020 (Working Group for the National Risk Assessment of Money Laundering, Terrorist Financing and Financing of the Proliferation of Weapons of Mass Destruction).

Glossary:

BACEN means Central Bank of Brazil;

CGU means Brazilian Office of the Comptroller General;

COAF means Council for Financial Activities Control, the Brazilian Financial Intelligence Unit (FIU) ;

CMN means National Monetary Council;

CNSP means National Private Insurance Council;

CVM means Securities and Exchange Commission of Brazil;

Regulatory Decree means Decree No. 11.129/2022, which regulates Law No. 12.846 (Anti-Corruption Law);

FINCEN means Financial Crimes Enforcement Network; and

FATF stands for the Financial Action Task Force, an intergovernmental body that sets international standards for Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT).

ICC stands for International Chamber of Commerce;

ISO 37002 is an international standard that provides guidelines for the implementation, operation, and continuous improvement of whistleblowing management systems;

KCIs stand for key control indicators;

KPIs stand for key performance indicators;

KRIs stand for key risk indicators;

OFAC stands for Office of Foreign Assets Control;

Anti-Corruption Law means Law No. 12.846/2013;

AML/CFT stands for Anti-Money Laundering and Counter-Terrorist Financing.

PREVIC means National Superintendency of Supplementary Pension;

SUSEP means Superintendency of Private Insurance;

US persons (United States Persons) mean individuals or entities subject to U.S. tax laws, including citizens (born or naturalized), Green Card holders, tax residents with substantial physical presence in the country, and companies/trusts incorporated in the United States; and

Wolfsberg Group is a voluntary association formed by leading international banks, dedicated to the development of global standards for anti-money laundering, countering the financing of terrorism, and responsible integrity practices in financial services.

Credits

This document is a Guide developed by ICC Brasil, with the support of the CGU. Its content does not necessarily reflect the individual opinions of the organizations that integrate ICC Brasil's network of relationships.

All Rights Reserved

ICC Brasil. Guide for Companies on Managing Risks Associated with Criminal Organizations. São Paulo: ICC Brasil, 2026.

This document was prepared with contributions from ICC Brasil member companies and coordinated by:

Executive Team

Gabriella Dorlhiac, Executive Director

Paula Costim, Head of Policy

Paula Scalco, Business Development Manager

Guilherme Rabel, Junior Policy Analyst

Leadership of the Integrity and Corporate Responsibility Commission and the Task Force on Integrity Against Organized Crime

José Alexandre Buaiz Neto, Chair of the Commission

Ana Paula Carracedo, Vice-Chair of the Commission

Chantal Pillet, Vice-Chair of the Commission and Task Force Co-Lead

Karina Martins, Vice-Chair of the Commission and Task Force Co-Lead

Carlos Flávio Lopes, Task Force Co-Lead

Paula Mader, Task Force Co-Lead

Luisa Mesquita, Task Force Coordinator

Marina Fronterotta, Task Force Coordinator

With the collaboration of CGU's Team:

Marcelo Pontes Vianna, Secretary for Private Sector Integrity

Cristine Köhler Ganzenmüller, Director for the Promotion and Evaluation of Private Sector Integrity

Monique Cerqueira Zuidema, General Coordinator for the Promotion of Private Sector Integrity

Sergio Filgueiras de Paula, General Coordinator for the Evaluation of Private Sector Integrity

Andre Spencer de Souza Holanda, Federal Auditor of Finance and Control

Isabella Brito, Head of Service of the General Coordination for the Promotion of Private Sector Integrity

Foreword

The impact of criminal organizations on business activities has become a central theme on the private sector's strategic agenda. This phenomenon directly affects the business environment, undermining corporate integrity and, consequently, competitiveness in Brazil and abroad. This risk is not limited to activities conducted in offices and corporate structures; it also extends to air, maritime, and land transport, making the topic particularly relevant to the debate on Brazil's business environment and its integration into international markets.

The increasing severity and complexity of this scenario evidenced the need for a deeper reflection and prompted ICC Brasil to launch a structured process of listening and dialogue with business leaders and the network of companies within its network. This mobilization, together with conversations involving representatives from different sectors, made it possible to better understand the main concerns, vulnerabilities, and constraints companies face when confronting this risk.

The information gathered throughout this process indicates that the actions of criminal organizations require companies to adopt more structured, detailed, and integrated approaches across their production processes. Such approaches can strengthen prevention, improve risk management, and enhance incident response across value chains. This context also highlights that addressing these threats demands strategic coordination between the private and public sectors, to deepen mutual understanding of the challenges involved and to foster the construction of collaborative solutions.

In this scenario, ICC Brasil, in collaboration with the Brazilian Office of the Comptroller General (CGU), developed this Guide. The publication, a result of the exchange of experience and knowledge between ICC Brasil members and the CGU, aims to support companies in understanding this phenomenon and strengthening their preparedness to deal with the potential presence and influence of criminal organizations in their operations. In doing so, it contributes to reinforcing compliance as a strategic instrument for protecting formal economic activity.

1 Introduction

The fight against corruption, money laundering, and criminal organizations constitutes a strategic priority for Brazil and Brazilian companies, as it directly impacts the real economy, the country's competitiveness and credibility, and public and private governance. Criminal organizations operate and expand their illicit activities by circumventing oversight and law enforcement mechanisms through various strategies, including the incorporation of seemingly legitimate business structures, the gradual acquisition or takeover of established companies, and the use of nominees to conceal the ultimate beneficial ownership of assets and operations.

These organizations are also involved in other illicit practices, such as money laundering, cargo theft, digital and environmental crimes, and infiltration into production chains. Because they maintain a facade of legitimacy, detection becomes significantly more complex. The infiltration of such practices compromises the reputation of countries and companies, challenges compliance structures, generates legal uncertainty, and weakens regulatory and economic stability.

Criminal organizations increasingly seek to infiltrate various public and private spheres to expand their influence and operations. For this reason, cooperation between the public and private sectors is essential to develop integrated, structured approaches to risk management.

In this context, the Guide for Companies on Risk Management Associated with Criminal Organizations aims to raise private-sector awareness of the presence and influence of criminal organizations in companies' production, supplier, and customer chains. The document also provides guidance to assist the management of risks associated with illicit practices affecting the formal economy.

Recognizing that the private sector plays a strategic role in identifying, preventing, and managing these risks, this Guide adopts a non-normative, non-exhaustive approach. Its objective is to present initial considerations and proposals on governance, incident management, and decision-making; examples of practical scenarios in which criminal organizations can infiltrate business operations; and reflections on the limitations and challenges companies face, particularly in compliance areas. These guidelines stem from the understanding that formal control and compliance mechanisms often encounter obstacles when confronted with the informal, asymmetrical, and transnational dynamics of criminal organizations.

The guidelines presented herein may serve as a reference for companies of all sizes and sectors, whether regulated or not, and whether directly or indirectly exposed to risks related to illicit activities. The application of the document presupposes adaptation to the specificities of each company, taking into account its business context, sector of activity, risk profile, and level of maturity in governance and compliance. The recommendations should be understood as proposals to strengthen internal processes for the identification and mitigation of these risks, rather than as definitive solutions, obligations, or binding standards.

The speed at which criminal organizations adapt is extremely high, underscoring the need for continuous monitoring and regular updating of the measures outlined in this Guide. This document organizes illustrative situations that can assist companies in addressing the topic. By identifying the problem and outlining possible measures to be adopted, this Guide serves as a reference for companies directly or indirectly exposed to the activities of organized crime.

2 Context, Diagnosis, and Nature of Risks

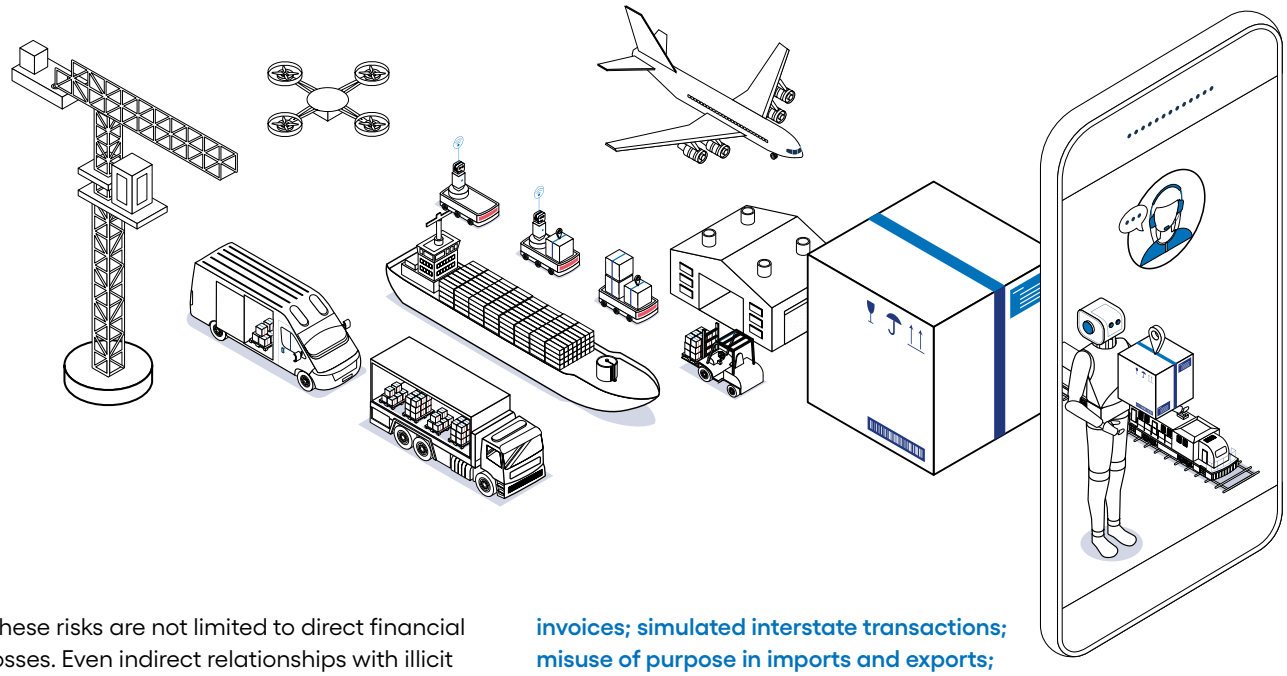
The Brazilian business environment has seen a significant increase in risks posed by the actions of criminal organizations. It is estimated that these organizations moved approximately R$ 350 billion between 2022 and 2024[1]. Therefore, this has systemic effects on tax revenues, competition, and market integrity.

As organized crime becomes increasingly bold and professionalized, it no longer limits itself to concealing illicit proceeds: instead, it seeks to infiltrate legitimate businesses, using complex corporate structures and entities as mechanisms for economic integration.

In this context, instruments such as investment funds, private equity structures, fintechs, holdings, offshore vehicles, M&A operations, franchises, and new service providers are being used not only to move funds but also to convert illicit capital into formal revenue, dividends, and capital gains, with an appearance of legitimacy. Criminal organizations are making greater use of legitimate means — such as mergers and acquisitions (M&A) — to launder or "legitimize" proceeds derived from criminal activities.

The structural infiltration of organized crime into legitimate businesses represents a significant systemic risk, as it favors money laundering, governance capture, distortion of competition, the economic influence of illicit groups, the normalization of illicit flows, and the compromise of company reputation and sustainability.

1 **FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA**. Follow the products: rastreamento de produtos e enfrentamento ao crime organizado no Brasil [product tracking and the fight against organized crime in Brazil]. Coordination: Nivio Nascimento; Eduardo Pazinato. São Paulo: Fórum Brasileiro de Segurança Pública [Brazilian Forum on Public Safety], 2025. Available at: https://publicacoes.forumseguranca.org.br/server/api/core/bitstreams/c5a85bb2-214a-4288-abf5-fcc619612777/content. Accessed on: April 6, 2026.



These risks are not limited to direct financial losses. Even indirect relationships with illicit activities can lead to financial losses and legal implications, as well as compromise companies' reputations, disrupt operations, weaken institutional integrity throughout the chain, and potentially endanger employees' safety. Recurring questions arise regarding how to map risk factors (red flags), monitor the market, identify signs of their materialization, engage the competent authorities, and act in a timely manner both within the business and with the involved counterparties.

The most frequent manifestations include tax evasion[2]; evasion of trade sanctions; money laundering; fraud; corruption; cargo theft and larceny; smuggling; intellectual property infringement and illicit trade of counterfeit products; misuse of logistical structures; and cyberattacks. Common practices adopted by criminal organizations include tax evasion through fictitious filings; sales without invoices; simulated interstate transactions; misuse of purpose in imports and exports; and structured delinquency, which includes shell companies, persistent tax debtors, and money laundering schemes.

Despite isolated advances by companies and oversight bodies, weaknesses persist in the adoption of broader, continuous preventive practices, particularly in identifying suspicious connections across the value chain.

Companies need to establish a structured and periodic risk assessment process, maintaining operational management instruments, internal controls, and effective mechanisms for monitoring potential red flags throughout the business value chain. This process should take as a reference, for example, risks of money laundering, corruption, misappropriation of assets, manipulation of accounting and financial information, and cyber risks, among others.

2 Tax evasion should be understood as a central dimension in the integrity agenda and in the fight against illicit flows. Criminal structures systematically resort to mechanisms such as tax evasion, underreporting of revenues, issuance of false invoices, interstate triangulation, and concealment of economic beneficiaries to artificially reduce their tax burden and finance illicit activities. The reduction of tax evasion, therefore, is not only a revenue-collection objective but also an essential component for mitigating competitive distortions, strengthening regulatory environments, and decreasing the economic space available to criminal organizations.

Among regulated companies, a higher degree of maturity is observed. These companies usually have formal compliance risk management structures, audits, documented policies, and regular communication and training programs. Even so, opportunities for improvement persist in expanding due diligence, conducting more in-depth analyses of potential partners, considering the specific characteristics of the regions where they operate, identifying ultimate beneficial owners, and enhancing the effectiveness and timeliness of third-party monitoring throughout the partnership or service provision, by the contracting parties themselves, in conjunction with their compliance structures.

In non-regulated companies, compliance and basic integrity functions are common. However, practices such as structured background checks and continuous monitoring are still applied only to a limited extent. The absence of specific protocols for critical situations, such as extortion or external threats, underscores the need to evolve toward more sophisticated prevention and response models.

Furthermore, attention devoted to money laundering risks remains limited. Many compliance programs continue to focus on anti-corruption topics or strictly reputational concerns. Aspects such as conflicts of interest, influence peddling, and criminal infiltration are often treated in isolation, even when they form part of the same risk dynamics.

An increase in co-optation of employees is also observed, often through high financial offers for strategic roles. The early identification of these situations is hindered by the lack of objective indicators, discreet identification and monitoring policies, the weak integration of compliance mechanisms into day-to-day business operations, a lack of trust in reporting channels, and the absence of clear employee protection protocols. Below, we present scenarios by sector and industry.

Industries:

- Specific vulnerabilities in transport, logistics, and outsourced services;
- Less visible access points that more easily escape traditional corporate controls;
- Risk scoring methodologies and continuous monitoring are still incipient (especially when compared to the financial sector);
- Long and fragmented production chains, characterized by multiple third parties and subcontractors;
- Operational heterogeneity across sites and regions;
- Data distributed across systems with low interoperability;
- Irregular quality of supplier information and low formalization;
- Increased risk of the unintentional receipt or movement of illicit proceeds; and
- Exposure to opaque corporate structures and hidden ultimate beneficial owners[3].

Fuel Sector

- Cargo theft and larceny;
- Adulteration, quality fraud, and volumetric fraud;
- Operation of clandestine blenders and mixers;
- Formation of cartels and other antitrust violations;
- Operation of "unlicensed" gas stations; and
- Increasing interest from organizations associated with drug trafficking.

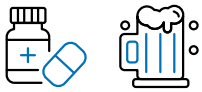
Forestry Sector

- Invasion of productive areas using heavy weaponry;
- Illegal land trading;
- Timber theft for clandestine charcoal production;
- Sending shipments to areas under criminal control, including as a way to test diversions associated with international routes; and
- Increase in attacks on cargo and attempts to contaminate containers in the port environment.

Financial Sector (banks and payment methods)

- Continuous exposure to illicit movements;
- Asymmetry between the adaptation capacity of criminal organizations and the resources allocated by companies for prevention and response;
- Impact of the professionalization of cybercrime; and
- Challenges associated with fintechs and the cross-cutting actions of criminal groups in different sectors of the economy.

3 Under the terms of Art. 53 of RFB Normative Instruction No. 2.290/2025, an ultimate beneficial owner is considered to be the natural person who, ultimately, directly or indirectly, holds ownership, exercises control, or has significant influence over the entity, as well as the natural person on whose behalf a transaction is conducted. The definition, therefore, adopts a material perspective aimed at identifying who effectively benefits from, commands, or influences the corporate structure or the operation, even if this position is not immediately revealed in formal documentation.



Medicines and Beverages Sector

- Intensification of counterfeiting, smuggling, and irregular circulation of regulated products;
- Parallel markets favored by the high economic value of the products;
- Expansion of unauthorized digital channels, making the tracking of operations difficult; and
- Growing concern regarding the diversion of inputs.

Product counterfeiting is a significant source of revenue for criminal organizations, often associated with other illicit practices such as money laundering, cargo theft and larceny, smuggling, and tax evasion. These groups exploit complex production chains, international logistics networks, and regulatory gaps to introduce counterfeit goods into the market, including through split shipments and decentralized production near consumer centers. According to OECD estimates, global trade in counterfeit goods reached approximately 2.3% of world imports, highlighting the scale and sophistication of these illicit activities[4].

Among the most affected sectors are clothing, footwear, leather goods, electronics, cosmetics, jewelry, toys, pharmaceutical products, vehicles, beverages, and food. In the Brazilian context, cases of adulteration of alcoholic beverages stand out, posing risks to public health, as well as fraud involving agricultural inputs, such as adulterated fertilizers, which can jeopardize productivity and, consequently, affect food security[5]. Counterfeiting affects both consumer goods and other products protected by intellectual property rights. In addition to economic losses and impacts on market integrity, the circulation of counterfeit products poses significant risks to customer health and safety, especially in the pharmaceutical, cosmetic, food, toy, and automotive parts sectors. This phenomenon compromises fair competition, weakens regulation and oversight mechanisms, and undermines trust in consumer relations.

4 **ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD); EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE (EUIPO).** Mapping Global Trade in Fakes 2025: global trends and enforcement challenges. Paris: OECD Publishing, 2025. Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/05/mapping-global-trade-in-fakes-2025_5c812e3c/94d3b29f-en.pdf. Accessed on: April 6, 2026.

5 **BRASIL**. Ministério da Justiça e Segurança Pública [BRAZIL. Ministry of Justice and Public Security]. Nota oficial — Sistema do Governo Federal registra nove casos de intoxicação por metanol [Official Statement - Federal Government System records nine cases of methanol poisoning]. Brasília, DF, September 26, 2025. Available at: https://www.gov.br/mj/pt-br/assuntos/noticias/nota-oficial-2014-sistema-do-governo-federal-registra-novecasos-de-intoxicacao-por-metanol. Accessed on: April 6, 2026; **BRASIL**. Ministério da Agricultura e Pecuária [BRAZIL. Ministry of Agriculture and Livestock]. Mapa apreende mais de 5 mil litros de fertilizantes irregulares no interior de São Paulo [MAPA seizes more than 5,000 liters of irregular fertilizers in the countryside of São Paulo state]. Brasília, DF, March 26, 2026. Available at: https://www.gov.br/agricultura/pt-br/assuntos/noticias/mapa-apreende-mais-de-5-mil-litros-de-fertilizantes-irregulares-no-interior-de-sao-paulo. Accessed on: April 6, 2026.

Furthermore, it is important to highlight that in **labor-intensive sectors**, corrective actions may lead to the demobilization of suppliers and the termination of contracts — measures that, in addition to compromising the continuity of operations, affect entire chains and produce relevant social impacts. Mitigating measures are important to avert the risk of demobilization and its consequences.

Since 2022, the main illicit financial flows have been concentrated in four areas: illegal fuel trading (R$ 61.4 billion), illegal beverage trading (R$ 56.9 billion), illegal gold extraction and production (R$ 18.2 billion), and illegal trade in tobacco and cigarettes (R$ 10.3 billion)[6].

Other relevant sectors that deserve attention include car dealerships, the real estate market, construction companies, currency exchange offices, public transportation companies (such as buses), religious organizations, social public health organizations, waste collection services, mining, betting companies, infrastructure, port services, and entities linked to soccer clubs. Although some sectors are more relevant or vulnerable in the analyzed context, exposure to criminal organizations' actions is not limited to them and can affect companies in all sectors of the economy to a greater or lesser degree.

Given this context, the diagnosis is based on the recognition that the risks associated with criminal organizations are dynamic and pervasive. Prevention, detection, and response strategies must be continuously improved as new patterns of action and vulnerabilities become evident. The strengthening of corporate resilience depends on consolidating an ethical culture that treats the prevention of criminal organizations as an integral part of management and governance.

Critical Role of M&A and Investor Relations (IR)

As key components in governance and compliance controls aimed at preventing the infiltration of organized crime, the M&A and IR areas occupy sensitive positions regarding the entry of illicit capital and must act as the first line of defense and governance.

The evolution of organized crime indicates a paradigm shift: illicit capital has moved beyond mere concealment and begun to seek integration, scale, and influence within the formal economy across almost all sectors.

Criminal organizations have realized that they can increase their financial results while simultaneously making detection more difficult by operating as if they were part of the licit market.

The inability of companies to formulate the right questions about economic substance, governance, and conduct in their relationships with partners makes them vulnerable not only to regulatory risks but also to the progressive infiltration of their own corporate structures.

The management of risks associated with criminal organizations must focus closely on investors, guarantors, and financiers, as well as on the active oversight of suppliers and customers. Managing the risk of corporate capture by organized crime depends on the company's ability to question the reasonableness and economic consistency of operations, as well as to maintain a zero-tolerance stance toward structural opacity.

6 **FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA.** Follow the products: rastreamento de produtos e enfrentamento ao crime organizado no Brasil [product tracking and the fight against organized crime in Brazil]. Coordination: Nivio Nascimento; Eduardo Pazinato. São Paulo: Fórum Brasileiro de Segurança Pública [Brazilian Forum on Public Safety], 2025. Available at: https://publicacoes.forumseguranca.org.br/server/api/core/bitstreams/c5a85bb2-214a-4288-abf5-fcc619612777/content. Accessed on: April 6, 2026.

3 Governance Proposals for Risk Management

3.1. Proposals for the Governance and Compliance Process

To outline measures to protect a company against risks that may affect its ability to achieve its purposes, it is particularly useful to revisit certain integrity-related concepts.

In recent years, specialized literature and government regulations have established the use of the term "integrity program" to refer to the set of internal mechanisms and procedures for integrity, auditing, and encouraging the reporting of irregularities, as well as the effective application of codes of ethics and conduct, policies, and guidelines. The objective is to prevent, detect, and remediate deviations, fraud, irregularities, and illicit acts, while fostering and maintaining a culture of integrity within the organizational environment. As a dynamic process, the integrity program must continuously adapt to new risks and contexts, which requires periodic reviews and the adoption of additional measures whenever necessary.

The CGU defines an integrity program as a set of internal integrity mechanisms and procedures, auditing, and incentives for reporting irregularities, as well as the effective application of codes of ethics and conduct, policies, and guidelines, with the objective of (i) preventing, detecting, and remediating deviations, fraud, irregularities, and illicit acts committed against the public administration, whether domestic or foreign; and (ii) fostering and maintaining a culture of integrity within the organizational environment, pursuant to Art. 56 of Decree No. 11.129/2022, which regulated the Anti-Corruption Law.

More recently, the concept of "integrity systems," developed by the Brazilian Institute of Corporate Governance (IBGC)[7], has gained traction. This concept views the integrity program as one component of a broader system, insofar as the system seeks to be a dynamic structure encompassing all internal units, programs, processes, activities, and policies that interact to ensure the company operates ethically and in compliance with its purpose, values, objectives, and applicable legislation.

7 **BRAZILIAN INSTITUTE OF CORPORATE GOVERNANCE (IBGC).** Sistema de integridade: fundamentos e boas práticas [Integrity System: Fundamentals and Best Practices]. São Paulo: IBGC, 2025. Available at: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=24725&assessment=1. Accessed on: April 6, 2026

Based on this approach, companies should consider not only strategies for in-depth analysis, dialogue, and auditing of evidence related to the provision of services and/or activities provided for in the contract, but also the strengthening of an ethical and integrity culture as a systemic process. This process should be endowed with adequate resources and capable of integrating different areas of the company to better anticipate and address unexpected consequences of known risks and those that may arise in new scenarios.

The integrity system is particularly useful in addressing the threat of criminal organizations. Unlike isolated illicit acts, criminal organizations operate through informal networks, personal relationships, and sophisticated concealment mechanisms that challenge traditional control models. In this scenario, **addressing the risk of criminal infiltration requires continuous dialogue and effective coordination across the company's different areas**. The management of this risk should not be assigned to an isolated unit: operational areas, especially those involved in contracting, payments, asset management, logistics, and third-party relationships, must be formally integrated into the prevention, detection, monitoring, and control system, with clearly defined responsibilities.

Senior management is responsible for establishing strategic guidelines, approving internal policies, providing adequate resources, and supervising their effectiveness, actively demonstrating their commitment and engagement toward institutional integrity. Areas responsible for compliance, integrity, or the prevention of illicit acts must operate with functional autonomy, direct access to higher decision-making bodies, and resources compatible with the level of risk exposure.

As a best practice for strengthening governance and increasing process reliability, it is recommended that companies evaluate adherence to certification programs and periodic audits, both promoted by internal structures and by sectoral associations and recognized entities. These voluntary mechanisms promote convergence toward minimum integrity and risk management standards, introduce independent verification procedures, facilitate peer-to-peer comparability, and reduce information asymmetries with customers, suppliers, investors, and authorities. Companies engaged in these initiatives tend to have more robust internal controls, greater transparency, and a lower propensity to engage in illicit practices.

In Brazil, the following initiatives undertaken by the Office of the Comptroller General (CGU) aimed at strengthening corporate integrity stand out:

Brazilian Pact for Business Integrity

Consists of a voluntary public commitment that encourages the adoption of corruption prevention measures and best governance practices, offering, among other benefits, a self-assessment tool that allows companies to diagnose the maturity level of their integrity programs.

Pro-Ethics Company

A recognition program for companies that demonstrate a commitment to the effective implementation of integrity programs through a structured evaluation process aligned with national and international best practices.

Participation in these initiatives can contribute to the continuous improvement of control mechanisms, adherence to recognized standards, and the strengthening of the entity's capacity to prevent, identify, and respond to risks associated with the actions of criminal organizations.

It should be emphasized that, beyond the adoption of internal policies and regulations, the structuring of integrity programs must consider the entity's culture, business environment, and exposure to risk. Such programs should not be limited to formal regulatory compliance, but to the establishment of a defense structure compatible with the sophistication of criminal organizations.

With the objective of increasing the company's protection against the actions of criminal organizations, instruments for defining standards of conduct, preventing money laundering, managing conflicts of interest, communicating and investigating irregularities, and, notably, managing risks associated with third-party relationships gain prominence.

In this context, practices include know your customer (KYC), know your partner or supplier, and the third parties they engage with in their service networks; know your employee (KYE); and, where applicable, other relevant relationships, such as investors and financial partners. These instruments must be carefully developed, formally approved, widely disseminated, and incorporated not only into the company's decision-making and operational routines but also into payment systems, so as to prevent the outflow of funds without due analysis. The same applies to periodic evaluations of effectiveness and efficiency.

This is because simple compliance with formal requirements does not, in itself, ensure the integrity of the process. Procedures such as the requirement for multiple quotes can be fulfilled by distinct companies that, in practice, are part of the same criminal structure, producing only an appearance of regularity. There is therefore a need to adopt an approach that goes beyond mere formal verification.

The formal mechanisms of compliance encounter structural limits in light of the specific dynamics of criminal organizations, which are guided by personal relationships of trust, coercion, economic dependence, and the constant adaptation and alteration of existing management and control instruments.

These structures frequently exploit the absence of clearly defined approval levels and limits, the lack of segregation of duties, the tolerance for procedural exceptions, the insufficiency of cross-checks, and, in many cases, the very lack of experience of the Compliance area in formulating effective responses, including in light of risks of creating animosities surrounding its operations.

Situations of "operational urgency," for example, can become a recurring justification for authorizations outside the normal flow, creating shortcuts that facilitate the insertion of illicit payments into legitimate processes. Likewise, the prolonged involvement of an employee in sensitive activities, such as supplier and customer registration or the validation of financial institutions, can foster the establishment of improper ties, compromising the independence needed to detect irregularities and facilitating the inclusion of shell companies in internal systems.

For this reason, the governance structure must incorporate complementary control mechanisms, such as the effective segregation of sensitive duties, periodic rotation in critical positions, the establishment of risk scenarios, periodic monitoring and analysis, the reinforcement of control over discretionary decisions, the performance of independent audits, the automation of controls, data cross-referencing, and the monitoring of atypical patterns of institutional behavior. In financial areas, for example, the concentration of supplier registration, approval, and payment execution in a single agent significantly increases the risk of criminal networks instrumentalizing internal systems.

It is also essential to establish secure internal or external (independent) reporting channels for indications of irregularities, accompanied by structured, transparent, and duly defined procedures for investigation, decision-making escalation, and the adoption of prevention, detection, and correction measures, whose combined strengthening is recommended. Protection against retaliation for good-faith whistleblowers and witnesses is a necessary element to break the dynamics of silence and fear frequently exploited by criminal organizations.

Thus, when an employee identifies that a supplier is repeatedly hired despite charging prices incompatible with market rates, the possibility of reporting the situation without fear of personal exposure can be decisive in interrupting cycles of illicit favoritism.

Finally, the effectiveness of governance and compliance in tackling criminal organizations depends on the consolidation of a structured institutional culture oriented toward integrity, which recognizes the levels and limits of formal controls and treats organizational vigilance as part of the business routine. The integration between areas, continuous training, and the consistent adoption of structural prevention and control mechanisms constitute conditions for increasing institutional resilience against criminal infiltration.

3.2. Minimum Policies and Procedures

To enable the practical and proportional implementation of the integrity program, companies are recommended to adopt a minimum set of policies and procedures aligned with their size, operational complexity, and level of sectoral and geographical exposure. This minimum standard shall ensure, at the very least:

Clear third-party due diligence guidelines, including ultimate beneficial owner identification;

Screening against public and private lists, Politically Exposed Persons (PEPs), and sanctions;

Financial controls with segregation of duties and bank account ownership validations;

Formal management of hiring and exceptions, with the recording of justifications and approval levels;

Continuous monitoring procedures based on objective risk triggers;

Reporting channels with effective protection against retaliation.

As a complement to internal implementation, the adoption of voluntary mechanisms for regular auditing and sectoral certification is encouraged, as they can validate the practical application of policies, test controls in critical processes, and attest compliance with recognized standards. This independent verification increases external credibility, provides additional institutional shielding, and expands the capacity to detect gaps, especially in environments with long supplier chains and multiple third parties.

In smaller companies or those with limited exposure, these controls may be smaller, prioritizing minimum documentation, double verification of registrations and payments, and traceability of decisions. In contexts of higher exposure, however, enhanced diligence is required for critical third parties, as well as integration with bureaus and public and private databases, automated alerts, and independent audits.

To guide the application of procedures, it is useful to adopt an operational checklist in simple language and incorporate it into daily routines. Thus, before the approval of a third party, the following must be minimally documented:

- Complete registration with CNPJ (National Registry of Legal Entities) validation;
- National Classification of Economic Activities (CNAE);
- Address and representatives;
- Identification and qualification of the ultimate beneficial owner;
- Verification of operational capacity compatible with the contractual scope; and
- Reputational screening against sanctions lists and confirmation of the ownership of the bank account designated for payment.

Prior to hiring, it is recommended to verify quote comparability and adherence to market prices, and to formalize integrity clauses. Prior to the first payment and any registration changes, technical validations must be conducted with segregation of duties among those who request, analyze, and approve, and any exceptions must be recorded with justification and approval by the competent authority.

Risk assessment can be supported by a set of guiding questions that facilitate the identification of red flags without relying solely on specialists. In situations involving a newly established supplier or one with minimal structure, it is advisable to confirm whether the declared capacity is compatible with the scope, whether there is a verifiable operational history, and whether there are shared corporate relationships, addresses, or attorneys-in-fact with other participants in the process.

In the event of atypical concentration of contracts in a short period or off-market prices, it is pertinent to evaluate the economic rationale, the presence of intermediaries without a clear function, and the existence of logistical or execution routes that deviate from the usual pattern. Finally, pressure due to urgency and requests for exceptions must be analyzed with caution. Similarly, in cases of requests for bank account changes, the ownership, supporting documentation, and the temporal proximity to significant payments must be investigated.

In smaller companies or those with more stable supplier chains, the combination of basic due diligence with ultimate beneficial owner verification, screening against sanctions lists, double-checking of registrations and bank accounts, and formal recording of exceptions tends to be sufficient as a starting point.

In medium-sized companies or those with moderate exposure, it is recommended to evolve toward a consolidated third-party risk map, enhanced due diligence criteria based on criticality, triggers for reassessment (corporate changes, change in subject matter or account, revenue peaks without operational explanation), sample audits, among others.

In large, regulated, or multinational companies, in addition to the previous measures, integration with relationship analytics, periodic parameter reviews, and stress tests[8] on critical suppliers are appropriate.

Considering resource limitations, the definition and application of controls must be guided by materiality and business impact, prioritizing processes and third parties whose potential risk may compromise operational continuity, results, regulatory compliance, and the company's reputation. To ensure effectiveness and continuous improvement, it is recommended to establish periodic metrics for evaluating the execution and performance of controls, allowing the measurement of their maturity level, identifying gaps, and providing feedback to the decision-making process, with the recalibration of diligence levels and the direction of investments to the points of greatest relevance and return in risk mitigation.

8 Stress tests in compliance consist of simulating extreme adverse scenarios, such as crises, fraud, or systemic failures, with the objective of evaluating the resilience of internal controls, the company's response capacity, and the effectiveness of prevention, detection, and remediation mechanisms, contributing to the strengthening of regulatory compliance.

3.3. Risk Management Proposals

Risk management aims to identify, assess, treat, monitor, and mitigate the risks to which the institution is exposed, taking into account the nature of its activities, its products and services, the profile of its customers, its operations, and the geographical areas of operation. As a point of reference, it is worth noting that the risk-based approach has already been applied in a consolidated manner to prevent corruption, money laundering, and terrorist financing. This history and knowledge can serve as a starting point and even as inspiration for building a model that specifically addresses the risks associated with organized crime.

The controls implemented must be proportionate to the identified risks. The risk methodology must be defined in advance and frequently reviewed. This is because a company's risk appetite often varies over time, as it is related to organizational strategy and business objectives.

In the risk identification process, at a minimum, **risks related to customers, products and services, geographical areas, and operational aspects must be considered**.

Regarding **customers**, factors such as the following must be assessed:

- PEP status;
- Residence or headquarters in jurisdictions classified as higher risk;
- The existence of complex corporate structures; and
- The engagement in cash-intensive economic activities.

Regarding **products and services**, the following should be observed:

- Cash transactions;
- International transactions;
- Products that enable anonymity or rapid movement of funds; and
- Non-face-to-face service channels.

Regarding **geographical risk**, countries or regions with deficiencies in their AML/CFT regimes and locations associated with organized crime must be considered.

In the **operational scope**, internal process weaknesses, the outsourcing of critical activities, and excessive dependence on automated systems without adequate human validation must be evaluated.

As mentioned, identified risks must be assessed based on objective, pre-established criteria, taking into account, at least, the probability of occurrence and potential impact, including financial, regulatory, reputational, and criminal aspects. Based on this assessment, risks must be classified, and their formalization and documentation are essential.

For the treatment and mitigation of classified risks, measures compatible with the identified level of exposure must be established, which may include, as the case may be, the limitation or refusal of certain operations, continuous and automated monitoring of transactions, periodic review of registrations, specific training for the most exposed areas, and the implementation of other additional control mechanisms.

The risk management system must be accompanied by indicators that allow for the evaluation of its effectiveness and timeliness. In this context, KPIs can be used, such as the percentage of updated registrations, the average time for alert analysis, and the volume of training conducted; KRIs, such as atypical increases in cash operations, growth in the number of clients classified as high risk, and the recurrence of alerts related to the same client; as well as KCIs, which allow for assessing whether control mechanisms are functioning adequately, that is, the effectiveness of internal controls. Examples of KCIs include the percentage of audited contracts, the number of compliance reviews conducted, and the average time to investigate reports.

AI tools can support risk management by automating the collection and integration of internal and external data, generating predictive indicators, and improving risk prioritization based on company-defined scenarios. The use of algorithms for sectoral, geographical, and behavioral risk analysis favors the dynamic updating of the risk matrix and the qualification of KRIs, provided they are backed by robust governance, with clear definitions of objectives and usage limits, data quality and timeliness criteria, periodic validation and testing, and monitoring of models and mechanisms that allow for understanding, auditing, and contesting results when necessary.

As mentioned, the risk matrix and risk management policies must be reviewed at least annually and whenever there are relevant changes in the business model, the introduction of new products or services, the occurrence of merger and acquisition (M&A) operations or other relevant corporate reorganizations, applicable regulatory changes, or the occurrence of relevant events such as fraud, sanctions, or reports of suspicious transactions to the competent authorities.

Finally, the importance of AML/CFT risk management governance can be cited, which must ensure clear definitions of responsibilities across the company's different areas, including senior management, the AML/CFT or compliance area, and operational areas.

Regarding partners, financiers, and guarantors, it is recommended to:

- Identify and validate the ultimate beneficial owner and the complete control structure of the investor or guarantor;
- Validate the source of funds;
- Map all transaction parties and structures to assess the absence of circular fund flows between the financier and the borrower (within the same economic group).
- Map structures involving credit use, guarantees, and securitization with artificial backing or recurring cash generation, which may generate interest and amortizations as “clean income”; and
- Validate the strategic rationale and the consistency of the valuation.

3.4. Proposals for Third-Party Due Diligence

Third-party due diligence is one of the central instruments of risk management, aiming to understand and help prevent companies' association with criminal organizations.

To conduct third-party due diligence processes effectively and consistently, it is essential to understand the mechanisms through which criminal organizations infiltrate the formal economy. In many cases, this infiltration is associated with the need to reintroduce illicit proceeds into the economic system, giving them an appearance of legality. This process generally occurs through money laundering, structured in three interdependent stages: i) the placement of funds into the economic system; ii) the layering (concealment) of their origin through multiple transactions; and finally, iii) their integration into apparently legitimate activities.

In this context, all third parties maintaining any commercial or operational relationship with the institution, including customers, suppliers, financial institutions, service providers, commercial partners, representatives, intermediaries, and consultants, must be subjected to due diligence procedures (known as Know Your Partner, Know Your Client, etc.), the intensity of which must vary according to the associated degree of risk.

The objective is to identify the structure, gain a better understanding of the third party, determine who exercises effective control over its activities, identify the economic beneficiary of the relationship (the ultimate beneficial owner), and verify whether the contracted activity has a legitimate economic purpose. Verifications to be conducted include reputational history, links with PEPs, and geographical exposure to criminal organizations.

Such verifications must also include the company's own employees and collaborators (Know Your Employee) to avoid the risk of co-opting professionals in sensitive areas, such as logistics, finance, and legal, whether through financial incentives or coercion in territories under the influence of criminal organizations.

Literature and cases analyzed by financial intelligence units reveal recurring patterns, such as newly incorporated companies without operational structure and the movement of large volumes of funds without economic substance. In view of this, third-party due diligence must include, at a minimum, the complete registration identification of the third party, its corporate structure, the identification of the ultimate beneficial owner of the relationship, potential political exposure, reputational history, and presence on restrictive lists9. The location where the third party operates must also be evaluated. Operations in regions of armed conflict, drug trafficking, or border areas may constitute a relevant risk.

Additionally, it is recommended to conduct structured cross-referencing of business information, including registration data, corporate history, links between partners and directors, addresses, and proxies, using internal and external databases. The use of specialized bureaus, as well as public and private databases, can strengthen the ability to identify corporate inconsistencies, shell structures, indirect relationships between third parties, and hidden ultimate beneficial owners, serving as an essential tool for detecting red flags and mitigating risks of criminal infiltration.

The compatibility between the service provided, the contracted amount, the evidence of the business relationship, and the third party's operational capacity must also be analyzed. The recent incorporation of a company that begins receiving high-value contracts without having a compatible structure to execute them is a relevant indication of risk, even if all formal documentation is in order. Another warning sign is the request to make payments related to the consideration for services into bank accounts held by a party other than the contracted third party.

9 The processing of personal data of third parties and employees shall comply with data protection legislation, especially the General Data Protection Law (LGPD), and be carried out in a lawful, proportional manner, limited to the purposes of anti-money laundering and countering the financing of terrorism (AML/CFT).

Data collection shall be restricted to the minimum necessary for identification, verification, and risk assessment, in accordance with the need-to-know principle. Processing must be supported by an adequate legal basis, notably the fulfillment of a legal or regulatory obligation and the regular exercise of rights. Data must be stored safely, with retention limited to the applicable legal periods, and disposed of securely and in a traceable manner after its purpose has been achieved.

The Data Protection Officer (DPO) must be involved in the definition and supervision of procedures, including risk assessment, the definition of legal bases, and incident response.

Data sharing shall occur exclusively within the limits of the law and for AML/CFT purposes, ensuring the confidentiality and transparency of information to data subjects, conditional upon applicable legal exceptions.

Thus, the main warning signs that companies should monitor regarding suppliers, customers, and other business partners can be organized as follows:

Corporate Structure

- Frequent changes of partners or directors without justification;
- Presence of partners with financial capacity incompatible with the company's revenue, such as beneficiaries of social income distribution programs[10];
- Partners without professional experience in the company's field of activity;
- Difficulty in identifying ultimate beneficial owners;
- Recently incorporated companies;
- Concentration of multiple CNPJs [National Registries of Legal Entities] at the same address; and
- Companies without a website or digital presence.

Financial Operations

- Excessive use of cash;
- International transfers without economic justification;
- Complex or circular financial flows;
- Accounting inconsistencies; and
- Inconsistency between amounts charged and market rates.

Operational Activity

- Lack of physical infrastructure compatible with the declared size (few employees, precarious facilities, lack of inventory);
- Company headquarters located at a predominantly residential address;
- Business volume incompatible with the operational structure;
- Hiring companies without a track record for significant contracts; and
- Declared company activity (CNAE) incompatible with the activities performed.

10 Relevant information can be obtained from the Transparency Portal of the Brazilian Office of the Comptroller General, which provides data on the relationship between companies and the Public Sector, as well as on the receipt of social programs by individuals.

Commercial Relationships

- Contracts with suppliers or customers without a verifiable track record or linked to individuals under investigation;
- Relationships mediated by third parties without justification;
- Unwillingness to provide documentation and information during due diligence; and
- Atypical transactions for the industry standard.

Organizational behavior or poor reputation

- Absence of an integrity program and structured governance practices;
- Resistance to accepting contractual clauses that imply the adoption of crime prevention mechanisms;
- Resistance to providing documents that allow for clarifying the company's status;
- Signs of weakness in internal controls or in the presented accounting records;
- Unusual urgency to close the deal.
- Inclusion in sanctions lists (such as CEIS, CEPIM, and CNEP or international lists, OFAC, European Union, World Bank, Inter-American Development Bank); and
- Negative media or the existence of multiple lawsuits.

Additional indicators

- Presence in vulnerable sectors (cash-intensive trade and services, fuel, foreign trade, transport and logistics, construction and infrastructure, private security, real estate market);
- Companies owned by offshore entities; and
- High financial risk resulting from assessments by oversight bodies or lawsuits.

Based on these elements, the third party must be classified by risk level. For third parties classified as higher risk, enhanced due diligence measures must be adopted, such as:

- Requesting additional documentation;
- Conducting interviews and on-site visits for validation;
- In-depth verification of the corporate structure;
- Approval by a superior hierarchical level and inclusion of specific integrity contractual clauses; and
- Continuous monitoring of the relationship.

It is noteworthy that the company should have a consolidated, integrated risk map of its third parties for their respective management.

Such enhanced due diligence measures are especially relevant because, in addition to reputational and financial impacts, the failure to identify or inadequately address red flags may expose the company and its directors to significant legal and financial risks. In certain circumstances, managers and those responsible for internal controls may be held liable when, having sufficient elements to identify irregularities, they fail to adopt appropriate measures within their sphere of action.

Despite their relevance, traditional due diligence processes face structural limitations due to the tactics of criminal organizations. The existence of valid business registrations, negative clearance certificates, and regular contracts does not prevent criminal structures from using formally incorporated companies to conceal the illicit origin of funds. For this reason, due diligence must be understood as a mitigation tool, not a risk-elimination tool. Even when properly conducted, residual risks persist regarding the adaptive capacity of criminal organizations and the asymmetry between formal controls and informal networks. A supplier initially considered low-risk, for example, may be used by a criminal group over time without an immediate change in its registration data.

To deal with these risks, third-party management must incorporate continuous monitoring mechanisms and action plans, including periodic updates of analyses, monitoring of relevant changes in CNPJ and registrations, changes in corporate control, share capital, or corporate purpose, verification of atypical transactions, reassessment of sensitive contracts, and the integration of risk information into the institution's decision-making processes.

The effectiveness of due diligence activities also depends on their integration with the governance and compliance structure. Information obtained in the third-party risk assessment should guide

hiring, payment, and contract renewal decisions, preventing the analysis from being reduced to a merely formal step detached from operational reality. When a third party begins to concentrate significant contracts without a clear economic justification, its status must be reassessed immediately.

Finally, the due diligence policy must expressly acknowledge its own limits and provide objective responses when, despite formal compliance with procedures, signs of illicit links arise. The adoption of a risk-based approach, combined with continuous monitoring and coordinated action across areas, especially with contracting areas and employees, is an essential condition for reducing the likelihood that the institution will be used by structures linked to criminal organizations.

Once a decision is made to proceed with the engagement of a third party, contracts must include specific clauses aimed at preventing and combating criminal organizations and money laundering, as instruments for risk mitigation and the protection of the integrity of business relations. The possibility of contract termination or suspension must be provided for in the event of red flags regarding the counterparty's involvement in criminal organizations or other illicit activities.

Contracts must also establish the obligation to immediately notify any change in corporate control, ultimate beneficial owner, or the accounts used for contract execution, and to prohibit subcontracting or assignment without the counterparty's prior consent.

Whenever applicable, conditions precedent to the contract's effectiveness must be provided for, including proof of licenses and authorizations, the procurement and maintenance of adequate insurance, and the demonstration of technical, operational, and financial capacity compatible with the contracted scope. Furthermore, contracts must include specific anti-corruption and anti-money laundering clauses that set out legal compliance commitments, require cooperation, and provide for contractual sanctions in the event of non-compliance, without prejudice to other applicable liabilities.

3.5. Proposals for Monitoring Mechanisms

Traditional monitoring models, based on fixed rules, static parameters, and predominantly ex post controls, present limitations in the face of the increasing sophistication of illicit schemes.

Public sources indicate that criminal structures organize themselves through:

- Shell companies;
- Simulated contracts or those lacking economic proportionality;
- Structuring and circular flow of payments (smurfing);
- Operations in cash-intensive sectors or those with high outsourcing;
- Long and opaque supply chains; and
- Intermediaries with low transparency regarding the ultimate beneficial owner.

These practices are disguised within apparently regular operations, making them difficult to identify through strictly transactional controls.

Classic models face recurring challenges. They rely on static parameters that are quickly outpaced by the evolution of illicit schemes, resulting in excess false positives, operational fatigue, and a loss of analytical focus. The fragmentation of information and dispersion of responsibilities persist among areas such as finance, procurement, logistics, commercial, and legal. In addition to this, there is the difficulty in capturing non-financial risks, such as:

- External pressures;
- Territorial influence;
- Atypical behaviors;
- Suspicious relational patterns; and
- Focus on isolated transactions to the detriment of identifying systemic patterns.

In this scenario, more integrated, risk-based approaches are necessary, with explicit recognition of the limitations of traditional controls.

The evolution of money laundering and the infiltration of criminal organizations reinforces the need for companies in the real economy, even when not required by law, to adopt proportional prevention and detection mechanisms, in line with the risk-based approach principle.

The structuring of an objective and proportional system starts with identifying vulnerabilities by mapping the processes and activities most susceptible to abuse or infiltration. Examples include:

- Procurement and contracting of critical third parties;
- Logistics and transportation;
- Cash management;
- Sub-contracting and local labor;
- Indirect channels;
- Resales and franchises;
- Commissioning and incentives;
- Donations, sponsorships, and institutional support; and
- Construction, expansions, and services provided in the field.

Based on this diagnosis, the company must define risk scenarios and behavioral typologies to guide ongoing management, with periodic reviews to incorporate changes in criminal patterns of operation.

An essential pillar is ensuring the traceability of what was done, by whom, and for what purpose through minimal standardized documentation of contracts, amendments, measurements, payments, and approvals, as well as clear recording of justifications for exceptions or decisions outside the usual flow. It is recommended to standardize, in a consistent manner, the minimum fields and records necessary for traceability, including:

- Contract or base agreement, amendment, or operational justification, when applicable;
- Supplier, CNPJ, and, when applicable, identification of the ultimate beneficial owner;
- Bank account or beneficiary bank details;
- Cost center or linked project;
- Reason for contracting or motivation for the decision;
- Who requested and who approved; and
- Any exceptions and respective justifications.

It is important that the records also state the presence of any intermediaries (brokers, commercial representatives, among others) who participated in the negotiation. Verbal or informal approvals must be avoided; decisions must be recorded in official channels, and exceptions must be fully documented with a record, justification, and appropriate supervision.

Companies with a degree of internationalization must assess exposure to international sanctions, especially when there are connection factors with specific jurisdictions, such as:

- Involvement of US persons;
- Payments in US dollars;
- Use of technologies or services of North American origin; and
- Inclusion in global supply chains.

In such cases, it is recommended to adopt proportional controls aligned with recognized references, such as OFAC and its sanctions program framework, as well as public risk guidance. Situations must be referred to the compliance area when, for example, a supplier is newly created (less than 24 months), an unusual corporate structure is present, or the ultimate beneficial owner is not clearly identified.

The effectiveness of monitoring depends on a clear workflow for handling red flags. A minimum process must include the definition of risk scenarios, as well as the stages of detection, qualification, recording, decision, and remediation.

Furthermore, it is essential to establish responsibilities and escalation criteria proportional to the identified risk, in alignment with financial crime risk governance frameworks, such as the Wolfsberg Group principles.

To support the design and calibration of alerts, the company may use official red flag libraries, such as FinCEN advisories, which are useful for identifying patterns associated with trade-based money laundering. Among the points of attention, the following stand out:

- Frequent changes in bank accounts;
- Amounts incompatible with the market;
- Existence of intermediaries without a clear function;
- Pressure for exceptions;
- Discrepancies between what was contracted and what was executed; and
- Recurring presence of unregistered third parties at the site of operation.

With the adoption of more sophisticated corporate structures and the apparent legitimacy of criminal organizations' operations, there is a growing need for intelligence tools, data integration, and predictive analysis to mitigate these risks. The focus on suspicious transactions remains relevant, but it is not sufficient on its own. It becomes necessary to observe relationships, patterns, and indirect connections, in line with recommendations on ultimate beneficial owner transparency. This includes:

- Mapping partners, directors, attorneys-in-fact, intermediaries, and representatives;
- Identifying shared addresses, bank accounts, telephone numbers, and links;
- Cross-referencing data from suppliers, sub-suppliers, and service providers; and
- Applying network analytics techniques to reveal hidden networks.

The use of Artificial Intelligence (AI) tools can strengthen continuous monitoring by expanding the capacity to identify atypical patterns and subtle correlations in a timely manner and to prioritize alerts by materiality and risk. Supervised and unsupervised models can support the detection of anomalies in payments, prices, and costs, as well as in logistics routes, registrations, and corporate changes, while network analysis techniques help reveal indirect connections between third parties.

Additionally, AI, when supported by a system for recording and retaining messages exchanged through corporate communication tools (e.g., email and phone calls), can help identify anomalies in interactions with counterparties.

The adoption of AI and the monitoring of corporate communication tools must observe principles of proportionality, traceability, and periodic performance review, preserving human oversight and data quality controls to avoid bias, reduce false positives/negatives, and ensure adherence to legislation (e.g., LGPD) and internal information security policies.

To increase the robustness of analyses, it is further recommended to integrate into monitoring routines information from:

- External bureaus;
- Public and private databases;
- Business registries;
- Commercial records; and
- Verifiable open sources.

The systematic cross-referencing of this data with internal records allows for:

- Identifying corporate inconsistencies;
- Atypical changes in control;
- Indirect links between third parties; and
- Patterns incompatible with the declared activity, contributing to the rapid and early detection of red flags.

To elevate analytical quality, more mature companies establish **integrated structures and multidisciplinary cells** that involve sales, procurement, finance/treasury, operations, corporate security, legal, and compliance.

Analytical technologies and alert automation support risk-based prioritization, outlier detection, and identification of complex patterns, provided they meet minimum maturity requirements, such as explainability, traceability, and periodic reviews, to avoid biases and loss of accuracy. Automation should complement, rather than replace, human judgment, especially in sensitive decisions.

Additionally, due diligence must go beyond onboarding and be triggered whenever triggers indicating a change in risk arise, such as:

- Changes in the corporate structure;
- Unusual changes in logistical routes;
- Revenue peaks without operational explanation;
- Successive contract amendments without economic rationale;
- Frequent changes of bank accounts;
- Pressure for exceptions outside the workflow; and
- Security incidents or local reports.

Simulations and stress tests make it possible to assess response capabilities in realistic scenarios, such as:

- Attempts to infiltrate critical suppliers;
- Coercion of local teams;
- Logistical fraud;
- Capture of hiring processes; or
- Internal leakage of sensitive information, strengthening preparation before the risk materializes.

Even robust programs face limitations, such as:

- Implementation and maintenance costs;
- Data quality and availability;
- Risks of algorithmic opacity;
- Need for trained teams;
- Information asymmetries and privacy restrictions; and
- Diverse and sometimes asymmetrical regulatory expectations for non-obligated companies.

Therefore, this set of measures must be understood as an evolutionary process integrated into governance, rather than an absolute guarantee against illicit risks.

3.6. Proposals for Training and Organizational Culture

A company's ability to identify and respond quickly to infiltration attempts by criminal organizations within its operations depends on the robustness of its formal controls and the quality of its organizational culture. In many cases, daily behaviors, team perceptions, and the internal environment determine whether a risk is perceived early on or remains invisible until it gains scale.

The first signs rarely present themselves as suspicious transactions. They usually arise subtly, through behavioral patterns, informal pressures, and small changes that, when normalized, evolve into structural risks. Recurring examples include:

- Acceptance of informal daily practices;
- Pressures to weaken controls;
- Use of intermediaries without a clear operational justification; and
- Organizational silence in the face of ethical or operational discomfort.

When these signals are not recognized and addressed, they become part of the routine, creating an environment in which risk becomes easily embedded and where formal controls, on their own, lose their capacity to respond effectively.

Conventional training, although necessary, has limitations. Frequently:

- They adopt excessively normative content distant from practice;
- They show low retention when long and occasional;
- They fail to address real dilemmas, where the answer depends on judgment and context; and
- They reinforce the perception that risk is the exclusive responsibility of the compliance area.

As a result, teams may complete formal training tracks and still fail to recognize weak signals in daily operations. More mature companies demonstrate that effective culture depends on intentionality, structured debate, and psychologically safe environments.

Implementing these initiatives requires a balance with business routines and priorities. Training and engagement actions, when excessive or disconnected from practice, can lead to overload or a loss of effectiveness. In this context, it is important for the company to monitor the knowledge absorption by the trained teams to evaluate the effectiveness of the actions and guide any necessary adjustments. Therefore, a gradual approach is recommended, proportional to the risk, integrated into existing processes, with leadership support, and focused on simple solutions applicable to daily life.

Another axis is the focus on weak and behavioral signals. Relevant risks tend to start with:

- Pattern changes;
- Informal pressures;
- Sudden changes; and
- Atypical conduct.

Training teams to perceive and report these variations increases preventive capacity and anticipates responses.

Engaged leadership is decisive. When leaders reinforce the importance of controls, transparency, and record-keeping, they reduce ambiguities and establish clear expectations. The consistent presence of leadership shifts the topic from a bureaucratic obligation to a management priority.

It is also essential to ensure safe spaces for dialogue and questioning. Environments in which employees can report questions and concerns without fear reduce zones of silence and broaden early detection. Culture is consolidated when ethics, risk management, and decision-making are embedded in concrete routines. Under this logic, compliance ceases to be merely a set of rules and becomes a guide to daily choices. A solid culture functions as a collective sensor, capable of perceiving risks before they reach the systems.

Even without sophisticated measures, certain actions already heighten perception and response capacity.

Specific training should be conducted with local leadership and the most exposed areas, such as:

- Procurement;
- Logistics;
- Construction and services;
- Commercial area and channels;
- Finance and treasury;
- Asset security;
- Legal; and
- Compliance.

The content should cover:

- Typologies relevant to the business;
- Red flags throughout the processes;
- Application of the exception policy;
- Minimum record-keeping requirements; and
- Escalation criteria.

Internal communication must translate concepts into operational reality, using recurring dilemmas such as "urgency," "referred supplier," and "bank account change." Simple narratives adapted to the company's context help demonstrate how deviations begin. Culture cannot be sustained if there is fear of reporting. Therefore, leadership must reaffirm the tone from the top, internal channels must ensure effective protection for whistleblowers, and the company must provide feedback on the status of reports. Without protection, there is no engagement. Without engagement, there is no culture.

To keep the culture active, continuous learning practices can replace extensive training. Microlearning, with short modules distributed throughout the year, tends to increase retention and immediate application of content, especially when complemented by brief, objective, frequent internal communications adapted to different audiences, reinforcing key messages and behavioral expectations. Scenario-based training, with simulations and role-plays, allows teams to practice responses to situations such as:

- Pressure to hire "referred" suppliers and employees;
- Out-of-flow urgencies;
- Undue external interference; and
- Attempts to obtain sensitive data.

These exercises, combined with targeted and recurring communications, reinforce learning, test escalation time, record quality, and adherence to defined workflows, thus contributing to the consolidation of the culture in daily operations.

The speak-up-by-design approach reinforces the idea that the culture should facilitate and normalize reporting, asking questions, and requesting help. This can be supported by quick clarification mechanisms, internal campaigns, and consistent feedback, in addition to objective protection against retaliation. Reporting should not be the exception, but the expected and encouraged behavior.

Integration with supply chain due diligence is also relevant, so that employees understand that internal conduct directly affects the integrity of suppliers, partners, and intermediaries.

Finally, culture indicators, such as KPIs and KRIs, allow for monitoring the volume and quality of reports, recurrence by area, concentration of exceptions, waiver rates, and the percentage of trained critical third parties. These indicators help measure maturity, identify blind spots, and prioritize actions.

This set of practices matters because culture acts as a living line of defense:

- Reduces blind spots;
- Anticipates risk perception;
- Strengthens local teams;
- Prevents the normalization of deviations;
- Improves monitoring quality; and
- Increases resilience in vulnerable environments.

Culture does not eliminate risk, especially in contexts of coercion, territorial informality, or power asymmetries, but it allows for earlier perception, faster reaction, and consistent risk treatment, reducing the likelihood of conversion into structural damage. Monitoring should be understood as an imperfect, evolutionary process integrated into governance, rather than an absolute guarantee against illicit risks.

4 Proposals for Incident Management and Decision Making

4.1. Proposals for Information Identification, Recording, and Preservation

Effective management of risks associated with criminal organizations requires a continuous cycle of:

01 Identification;

02 Recording;

03 Decision-making;

04 Qualification;

05 Detection;

06 Remediation;

07 Monitoring of evidence.

For the cycle to function, the company needs structural and consistent mechanisms to identify relevant signals, apply objective assessment criteria, maintain integral records, and preserve evidence, while systematically incorporating lessons learned over time.

In this context, the creation and maintenance of an organized red flag file is recommended to consolidate warning signs identified in internal processes, standardize analyses, guide decisions, and strengthen institutional memory. For each red flag, the source process, severity level, and expected conduct must be indicated. Examples include:

- Unidentified ultimate beneficial owner;
- Corporate changes without justification;
- Operations incompatible with declared capacity;
- Atypical use of logistical routes;
- Urgency requests without adequate documentation;
- Split or exception payments;
- Improper approaches to employees in critical roles; and
- Interactions with recognized sensitive regions or sectors.

For consistent capture and treatment, it is necessary to establish a structured integration workflow across compliance, legal, human resources, operations, and other relevant areas, with defined responsibilities and orderly information sharing to avoid fragmented analysis and context loss.

The qualification of information is also a determining factor. Verifiable information, such as documents, system data, and physical evidence, enables immediate analysis and, when necessary, rapid escalation. Preliminary reports, yet unproven, require plausibility checks, requests for additional evidence, and provisional classification. Finally, subjective perceptions and weak signals should be recorded concisely and used to enhance monitoring, as they may anticipate risks, especially when analyzed alongside other indicators.

The robustness of the process also depends on the proper preservation of records and evidence to ensure integrity, validity, and future utility. The following is recommended:

- Secure and traceable storage of records;
- Prohibition of any manipulation that compromises reliability;
- Restriction of access to directly involved personnel;
- Recording, whenever possible, of the chain of custody; and
- Adoption of retention periods compatible with the complexity of cases related to criminal organizations.

These precautions strengthen internal prevention and response capabilities and protect the company in the event of verification by authorities or external audits, by ensuring that decisions are anchored in robust, duly documented evidence.

4.2. Proposals for Internal Assessment and Escalation

As part of incident management and decision-making, once the identification, recording, and preservation of information related to the case are concluded, the institution must define how to assess and escalate the matter internally. As previously indicated, criminal organizations generate distinct exposures depending on the sector, location, size, and operational characteristics of each company. Thus, assessment and escalation may follow best practices but must be adjusted to each company's reality.

The assessment of compliance and governance issues, as well as the determination of the appropriate time for escalation, are sensitive points in corporate governance. In situations involving criminal organizations, this sensitivity increases, as **infiltration tends to occur gradually and in a fragmented, informal manner, exploiting information asymmetries, territorial pressures, economic dependence, and operational gaps**. As a rule, the company does not initially encounter conclusive evidence or fully proven facts.

Criminal organizations deliberately exploit "gray areas" of business decision-making, in which isolated signals are treated as insufficient or merely operational. These dynamics delay institutional responses and allow the risk to consolidate over time. Criminal networks also benefit from hesitation in the face of incomplete information, using formally regular companies to access contracts, financial flows, and legitimate logistical chains.

Without timely escalation, relationships consolidate, create operational dependence, and broaden the risk of using logistical infrastructure for illicit activities.

In the financial system and payment methods, for example, public investigations have shown the use of formally active companies for transactions incompatible with their declared economic activity. Initial alerts regarding split transactions, opaque corporate links, or atypical movements are sometimes placed under passive monitoring, delaying more restrictive internal decisions and allowing the continued use of these structures for money laundering.

Infiltration is also observed in procurement processes, where distinct companies participate in quotes or tenders, formally meet the requirements, and yet maintain indirect links with partners, representatives, or addresses.

When analyzed in isolation, these elements do not trigger escalation, favoring the appearance of regularity and the prolonged permanence of structures linked to criminal organizations within corporate systems. A modus operandi previously interpreted as “mere fraud or collusion” may, in certain contexts, represent an entry point for criminal networks.

In regions under the influence of criminal groups, informal employee reports of external pressures or “recommended” suppliers are often disregarded due to a lack of documentary evidence. However, coercion is a frequent part of the acting method and, by its nature, tends not to leave formal records that can be presented as evidence. Signals classified as subjective may constitute relevant vectors of the progressive infiltration into operations.

In light of this scenario, internal assessment should not rely on a binary logic of confirmation or dismissal. It is a continuous exercise in risk management, with the adoption of measures proportional to the identified exposure, even in an environment of uncertainty. Experiences documented by Financial Intelligence Units and by European authorities reinforce the utility of distinguishing, within the decision-making process, between **verifiable facts, objective evidence, and analytical hypotheses**.

Facts consist of direct evidence, such as documents, system records, transactional data, and physical evidence.

Evidence corresponds to consistent information not yet fully confirmed, such as repeated reports, atypical patterns, or monitoring alerts.

And **hypotheses** are interpretations constructed from these elements, which guide additional due diligence and containment measures.

This distinction reduces the risk of decision-making paralysis and prevents rushed responses. However, the sufficiency of information for prevention and mitigation purposes should not be confused with the evidentiary standard required for criminal or administrative liability. Within the scope of corporate governance, the central question is whether the available elements justify reasonable measures to reduce exposure, preserve evidence, and prevent the continuity of potential illicit practices.

Prioritization and escalation should consider, in an integrated manner, two axes: **potential severity and urgency**.

Severity involves the magnitude of legal, regulatory, financial, reputational, and operational impacts, with special attention to the safety of personnel and assets.

Urgency arises from the time available to act before the risk worsens, whether due to the dissipation of relevant information, the need to continue payments, the execution of sensitive contracts, or the exposure of field teams.

Situations indicating possible access by criminal organizations to critical processes, such as logistics, transport, security, asset management, supplier registration, and information technology, require increased attention, even when the initial amounts involved are not significant.

Escalation should be understood as a mechanism for institutional protection, rather than an automatic recognition of wrongdoing. By submitting sensitive situations for analysis by higher instances or multidisciplinary committees, the company improves decision quality, reduces individual biases, and ensures decisions guided by multiple perspectives, in line with best practices for governance and risk management.

The absence of clear criteria tends to favor two recurring deviations identified in public investigations: (i) prolonged inaction in the face of relevant risks under the argument of lack of evidence; and (ii) the adoption of abrupt and disproportionate measures, with significant operational impacts and side effects. Internal protocols, even if flexible, provide predictability, consistency, and traceability to decisions.

Certain situations warrant immediate escalation, regardless of the investigation's stage. Among them are:

- Signs of coercion;
- Extortion or threats to employees;
- Signs of infiltration into critical processes, attempts to conceal or destroy information;
- Explicit pressure for hiring or payments outside the regular workflow;
- Suspicious changes to bank beneficiaries; and
- Significant exposure to transnational crimes, such as smuggling and trafficking.

In these cases, the protection of personnel, the preservation of evidence, and risk containment must prevail over strictly operational considerations.

Furthermore, initial measures should, whenever possible, prioritize precautionary and reversible responses, such as:

- Temporary suspension of payments;
- Expansion of due diligence;
- Restriction of access to systems and facilities; and
- Review of critical routes or suppliers.

The governance of the decision-making process requires clarity of roles and responsibilities. Technical assessment should be conducted by qualified personnel, with autonomy and access to relevant information. Decisions with significant material impact must involve senior management, in accordance with the company's governance structure.

The documentation of decisions, including the recording of elements considered, alternatives evaluated, and justifications adopted, constitutes an essential practice for auditing, institutional learning, and any interaction with authorities.

Finally, international experience demonstrates that decisions regarding the interruption, replacement, or continuity of commercial relationships potentially exposed to criminal organizations involve complex trade-offs between security, financial impact, social responsibility, and reputation. Recognizing these limits in advance, establishing clear escalation criteria, and aligning expectations at the leadership level reduce ad hoc improvisations under pressure and strengthen institutional resilience.

Thus, internal assessment and escalation must be understood as central instruments for anticipating risks, responding proportionately, and preserving integrity, personnel, and operations in complex environments where the actions of criminal organizations continuously challenge formal controls.

4.3. Proposals for Internal Reporting Channels

It is important to highlight that, in identifying potential suppliers linked to criminal organizations, the effectiveness of internal reporting channels depends on structured guidelines that mitigate channel underutilization, fear of retaliation, and confidentiality weaknesses. These guidelines are not limited to the formal creation of a reporting channel but encompass its governance, operationalization, and integration into the corporate integrity system to function, in practice, as an instrument for prevention, detection, and response. Its design must therefore be aligned with the parameters of trust, accessibility, and whistleblower protection.

Third-party access to the reporting channel, on the other hand, constitutes one of the main obstacles to the effectiveness of the global reporting, investigation, and remediation process. In complex production chains, commercial partners are often not fully integrated into the company's integrity culture, hindering the dissemination, understanding, and trust in reporting mechanisms. The problem tends to worsen when suppliers and service providers are unaware of the reporting channel, face overly complex report mechanisms, or fear commercial consequences resulting from a report, thereby significantly reducing the likelihood that irregularities are communicated in a timely manner.

Therefore, it is essential to widely publicize reporting channels in clear, accessible language, ensuring they can be used by employees, directors, service providers, and other third parties in the supply chain. It is also necessary to establish transparent internal procedures for the receipt, screening, investigation, and closure of reports, so as to strengthen the mechanism's credibility and encourage its responsible use.

Fear of retaliation is one of the main inhibiting factors when a report involves suspicions of criminal organization infiltration in strategic suppliers or relevant partnerships. In such cases, the perception of personal, asset, professional, or reputational risk can reduce the willingness to report illicit conduct or signs of irregularity, compromising the channel's preventive purpose.

In light of this, it is recommended to adopt explicit non-retaliation policies, accompanied by monitoring and accountability mechanisms that can identify and sanction retaliatory practices, including indirect or veiled ones. Whistleblower protection must be treated as a central element of risk mitigation, as it enables a continuous flow of relevant information for corporate integrity management.

Given the criticality of reports on potential criminal organization involvement, preserving the reporter's identity is essential to maintaining the channel's legitimacy and trust.

In accordance with ISO 37002, it is recommended to adopt tools that allow for anonymity and ensure the confidential treatment of cases, with access restricted to professionals responsible for the investigation, ensuring compliance with the principles of necessity, purpose, and proportionality.

Proper confidentiality management also requires clear criteria for the internal and external sharing of reported information, especially when communication with authorities is required. This sharing must be conducted responsibly and in a manner that protects the reporter's identity and the integrity of the investigations, avoiding exposure that compromises the safety of those involved and the effectiveness of the measures adopted.

Finally, strengthening reporting channels is not merely a procedural measure but a risk-mitigation strategy to address the company's exposure to indirect links with criminal organizations, with implications for legal liability, governance, and institutional sustainability.

4.4. Proposals for Reporting to Competent Authorities

Within the scope of mitigating risks arising from criminal organizations' actions in business relationships, reporting to competent authorities may be a relevant and necessary measure for the company, depending on the nature and severity of the identified situation.

Unlike internal mechanisms, external communication involves sharing information with state bodies, such as police authorities, the Public Prosecutor's Office, regulatory agencies, and oversight bodies, with potential legal, reputational, and operational consequences. In this sense, external reporting can create uncertainties about the timing, extent, and most appropriate form of communication, especially when the facts are still in the early stages of an internal investigation.

Brazilian legislation encourages cooperation between the private sector and public authorities, leaving companies to assess the most appropriate form and timing for any potential communication. This decision must consider, among other elements, the robustness of the available evidence, the risk of the illicit practice's continued existence, the threat to employees' physical integrity, the potential involvement of public agents, and the incidence of specific regulatory obligations.

In this scenario, the Anti-Corruption Law and its respective Implementing Decree, by valuing effective integrity programs, reinforce the importance of diligent, structured, and good-faith performance. Thus, the careful assessment of available information and the circumstances of the case helps ensure that any communication to authorities is conducted responsibly and in a timely manner.

Omission in the face of consistent evidence of supplier or customer involvement with criminal organizations can be interpreted as a failure of diligence and risk management, especially when the company maintains business relationships potentially tainted by illicit practices. In such cases, external reporting may be necessary to mitigate systemic risks and demonstrate institutional commitment to legality, thereby preserving objective good faith.

The appropriate conduct of the communication process contributes to preserving institutional credibility and image, without prejudice to cooperation with competent authorities. The decision on whether to communicate with authorities must also take into account potential reputational repercussions, including the form, channels, and institutional communication strategies, considering the information's sensitivity and relevance.

Therefore, an individualized assessment of each case is recommended. Factors to be considered include, among others, the nature and consistency of the evidence, the degree of involvement of counterparties and internal employees, the risks of continuing the commercial operation, the possibility of concealment or destruction of evidence, and the potential developments of ongoing investigations. This assessment can be conducted by qualified internal bodies, such as legal and compliance departments, to ensure decisions are consistent with the company's integrity strategy. The adoption of internal protocols for external reporting, the definition of responsibilities, and structured decision-making flows, with proper legal counsel, reduces arbitrariness and provides predictability to the decision-making process.

External communication may be necessary to disrupt more serious illicit activities, mitigate systemic risks, or support investigations of public interest. Still, the decision on whether to communicate with authorities must take into account the sensitivity of the topic, primarily to ensure that, if communication does occur, it is appropriate and proportionate. As a rule, reporting is advisable when there is consistent evidence of illicit practice, a concrete risk of recurrence, the possibility of evidence destruction, or a potential significant impact on third parties, the market, or the public administration.

From this perspective, responsible cooperation with authorities, when aligned with an effective integrity program, helps reduce exposure to legal and reputational risks arising from criminal organizations' influence on commercial relationships.

Fala.BR Channel and reporting to authorities

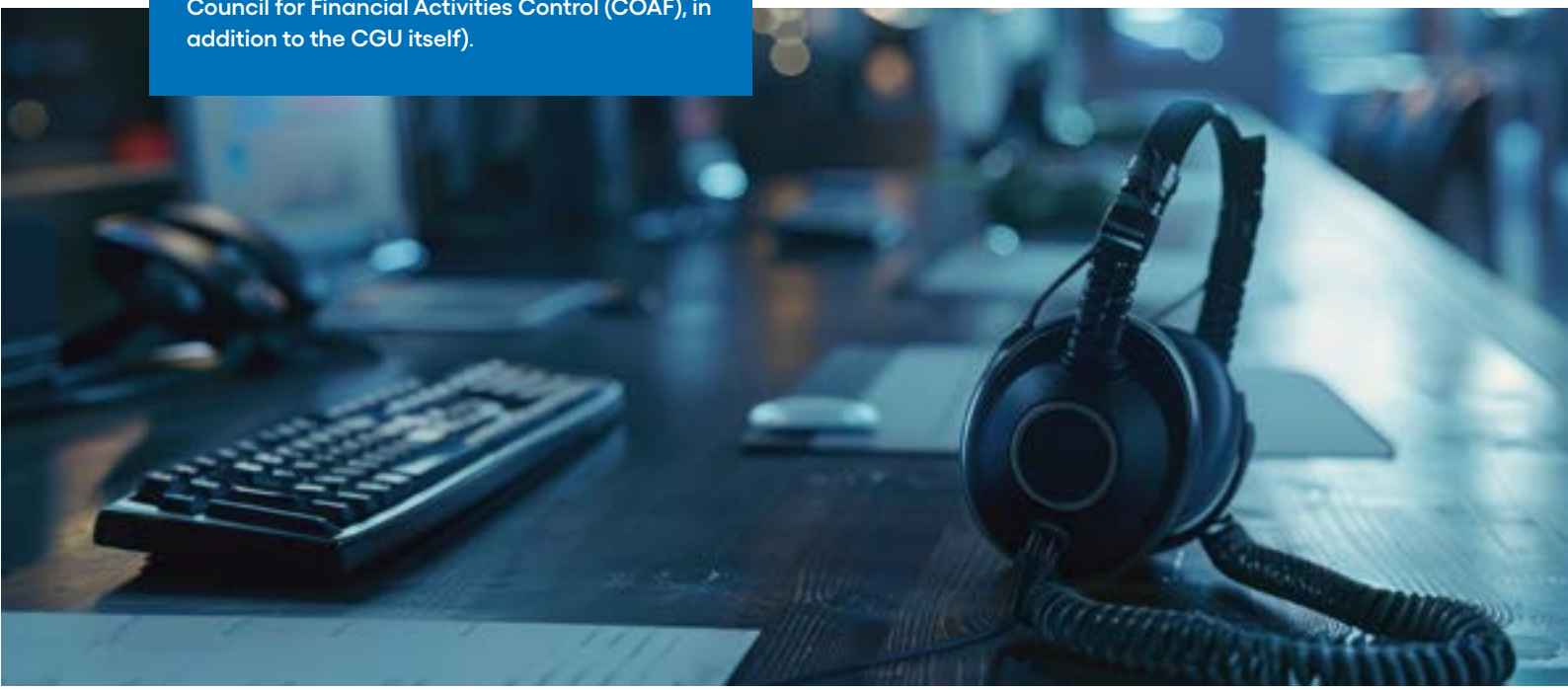
One of the channels that companies and employees can use to report situations related to potential irregularities or signs of criminal organization activity is the one provided by the CGU.

Fala.BR (falabr.cgu.gov.br) is the official platform for receiving and processing reports, including anonymous ones, with mechanisms designed to protect the whistleblower's identity. Submissions can be made by individuals or legal entities, with the possibility of tracking through the Gov.br account, in addition to sending detailed information and attachments to assist the investigation.

The system adopts protective measures such as identity confidentiality (when provided), data access restriction, and the possibility of anonymous registration. Reports are assessed for consistency and may be forwarded to the competent bodies for investigation. It is not necessary to present evidence, but providing complete information contributes to the effectiveness of the analysis. When making a report, it is possible to select which body or entity the submission should be sent to **(Examples include: Federal Police, Federal Highway Police, Council for Financial Activities Control (COAF), in addition to the CGU itself)**.

Furthermore, one must not lose sight of situations in which criminal organizations' actions pose a risk to employees' physical integrity, whether through threats or the commission of criminal activities on the company's premises or using its resources. In these hypotheses, it is essential to have a specific protocol for risk assessment and secure communication with police authorities.

Although the previously mentioned considerations regarding the timing and form of reporting also apply, urgent situations may require immediate communication to the State. For this reason, it is recommended that the company previously map the available channels for reporting and notifying of crimes in the locality. In this regard, it is worth mentioning other national reporting channels maintained by the public sector. Highlights include **Disque-Denúncia (181)**, widely used for the anonymous reporting of crimes, especially at the local level; **Comunica PF**, a Federal Police channel for receiving information on federal crimes; **Disque 100**, focused on reporting human rights violations; and **Ligue 180**, a specialized channel for assisting and referring cases of violence against women.



4.5. Proposals for Protection Measures, Business Continuity, and Crisis Management

Mitigating impacts and preserving business continuity in the face of risks posed by criminal organizations requires an integrated, proportional, and evidence-based approach.

The protection of personnel and essential assets must constitute the first axis of any response. Security protocols should guide employees operating in higher-risk regions, routes, or with higher-risk counterparties, with guidelines for safe and, where necessary, discreet conduct, to reduce vulnerabilities and the risk of retaliation. Depending on the severity, measures such as temporarily removing threatened employees or those involved in sensitive situations may be adopted.

Continuity of operations, while preserving integrity, requires that business operations do not entail any relaxation of ethical standards or compliance requirements. In environments with criminal groups, for example, it is recommended to map and activate alternative supply and logistics routes, even if this entails replanning and additional costs. Similarly, third parties associated with consistent signs of irregularity must be replaced temporarily or permanently based on objective criteria of severity and materiality, even when there is a significant operational impact. Regarding critical processes, contingency plans must provide for minimum service levels, degraded operation, and previously tested parallel routes. Thus, the periodic review of geographical, sectoral, and behavioral risks must be integrated into planning so that emerging vulnerabilities are not addressed solely reactively.

In the same vein, the crisis management process must be structured with knowledge of scenarios related to third-party risks, to ensure effective responses and careful, objective, coordinated, and consistent internal and external communication.

It is also important that sensitive information does not circulate informally to avoid distortions, undue alarm, or exposure of employees and assets. Internally, frontline teams must receive objective, targeted guidance on conduct, reporting channels, and escalation procedures. Externally, clients, partners, and other stakeholders must be informed in a factual and proportional manner, preserving confidentiality when required by law or by the integrity of the investigation, under legal guidance. Premature or contradictory communications hinder decisions and erode trust; therefore, communication discipline is an integral part of the response itself.

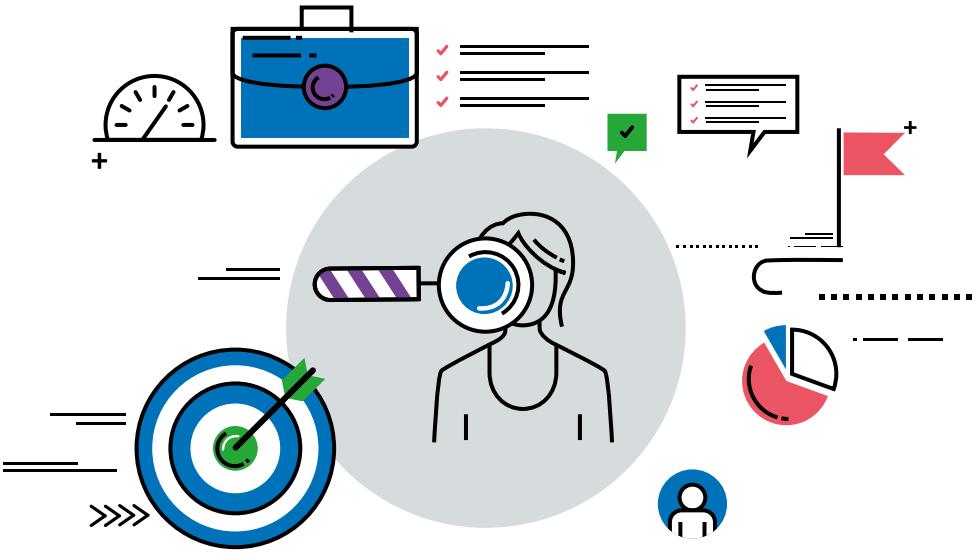
In scenario planning and in recognizing operational limits, it is necessary to acknowledge that, even with robust protocols, a company's intervention capacity is limited in territories under the influence of criminal groups. Information may be incomplete or based on local perceptions, and decisions involve hard choices between safety, financial impact, and reputation. The company's role is not to replace the State, but to act responsibly within its sphere of control, with the support of external specialists and coordination with competent authorities when necessary. Definitions of loss limits, escalation triggers, and criteria for suspending, reducing, or relocating operations must be agreed upon in advance and reviewed in light of lessons learned.

In short, the assessment of indirect and collateral effects must be continuous and multidisciplinary. The demobilization of local suppliers can produce socio-economic impacts on vulnerable communities. The substitution of routes or counterparties can increase field teams' exposure. Unmapped dependencies in the supply chain may emerge after interventions. Furthermore, both action and inaction can generate significant reputational effects. Therefore, decisions must incorporate perspectives from across compliance, operations, security, and procurement, with periodic impact reviews and, when applicable, social and operational mitigation measures.

Finally, a preventive stance and organizational culture are as relevant as technical controls. The company must foster an environment in which early reporting is valued, fears of retaliation are reduced, and transparency is reinforced by exemplary leadership.

It is also necessary to make explicit that difficult decisions in favor of integrity have the effective support of senior management, so that the principle of "continuing to operate ethically" prevails over deadline, cost, and market pressures. In this context, it is equally important to consider that performance metrics based exclusively on production or analysis volume may discourage attention to signs of fraud and reduce team adherence to practices for reporting irregularities or suspicious situations.

A preventive culture, post-incident learning, updates to the red flag library, and continuous workflow improvement increase corporate resilience and protect people, assets, and reputation, preserving continuity without wavering on principles.



5 Final Proposals

This Guide offers initial references for corporate reflection regarding a better understanding and the mitigation of risks associated with the actions of criminal organizations in business and commercial relationships, recognizing the complex and asymmetrical nature of this phenomenon. Such risks go beyond direct financial losses, extending to reputational impacts and, in certain contexts, to the safety of people and assets. The Guide does not replace legal or regulatory advice, which is fundamental for this type of topic. Business decisions must prioritize protecting people, assets, integrity, and legal compliance, especially in high-risk or information-uncertain contexts.

The proposals presented stem from the recognition that there are no one-size-fits-all or definitive solutions. The effectiveness of prevention, management, and response measures depends on an organization's ability to adopt approaches proportional to its risk profile, to integrate governance, compliance, operations, and organizational culture, and to continuously review its mechanisms in light of the ongoing advancement and refinement of criminal organizations. Formal controls reveal their limits when they lack senior management commitment, cross-functional cooperation, and an institutional environment that prioritizes the identification and timely treatment of red flags.

In this context, the relevance of adopting robust third-party risk management governance is highlighted, establishing and requiring the necessary documentation, the rationale, and the traceability of decisions, the strengthening of the mapping of higher-risk counterparties and operations, the promotion of trust in internal reporting channels, the protection of employees, and the adoption of mitigation measures proportional to the identified risks. Incident management and decision-

making must be understood as processes for addressing unpredictability and balancing safety and integrity with business continuity. This set of challenges demands continuous commitment from governance bodies and senior management, investment in training and monitoring tools, integration between areas, and institutional learning.

This document was prepared within the scope of the Integrity and Corporate Responsibility Commission of ICC Brasil, the national chapter of the ICC, an organization that institutionally represents more than 45 million companies in over 130 countries. ICC Brasil brings together its members in eight thematic commissions and seeks to contribute to the formulation of public policies aimed at the country's socio-economic development through continuous dialogue between the public and private sectors.

The Integrity and Corporate Responsibility Commission's mission is to strengthen the culture of ethics and integrity within organizations and to contribute to the continuous improvement of the national regulatory environment. Its work is focused on combating corruption and promoting ethics and integrity as fundamental pillars of reputation, trust, and competitiveness.

The preparation of this Guide included the collaboration of the Secretariat for Private Sector Integrity of the Brazilian Office of the Comptroller General (CGU), which has the authority to act across three areas: the promotion, regulation, and evaluation of integrity programs; the accountability of legal entities for illicit acts; and the execution of leniency agreements with legal entities committed to remedying harmful acts, improving their integrity measures, and assisting the Public Administration in the investigation of illicit acts and recovery of misappropriated assets.

Checklist

1. Governance and Compliance

- ☐ Senior management has established strategic guidelines, approved internal policies, and supervised their implementation regarding criminal organization risks.
- ☐ Areas responsible for compliance, integrity, or the prevention of illicit acts operate with functional autonomy, direct access to higher decision-making bodies, and possess resources compatible with the level of risk exposure.
- ☐ The management of criminal infiltration risk is not assigned to an isolated unit: operational areas (procurement, payments, asset management, logistics, and third-party relationships) are formally integrated into the prevention system, with clearly defined responsibilities.
- ☐ The company maintains continuous dialogue and effective coordination between different company areas to tackle the risk of criminal infiltration.
- ☐ There is a structured and comprehensive risk assessment process, with defined management instruments, internal controls, and effective monitoring mechanisms throughout the value chain.

---

2. Third-Party Due Diligence

- ☐ All third parties maintaining a commercial or operational relationship with the company (customers, suppliers, service providers, commercial partners, representatives, intermediaries, and consultants) are subject to due diligence procedures.
- ☐ Due diligence includes, at a minimum: complete registration identification, corporate structure, ultimate beneficial owner identification, potential political exposure, reputational history, and presence on restrictive lists.
- ☐ The location where the third party operates is evaluated, especially in regions of armed conflict, drug trafficking, or border areas.
- ☐ There are continuous monitoring mechanisms, including periodic updates of analyses, monitoring of changes in CNPJ and registrations, and changes in corporate control, share capital, or corporate purpose.
- ☐ Split payments, prices incompatible with the market, or sudden changes in bank beneficiaries are treated as red flags.
- ☐ Information obtained in third-party assessments guides hiring, payment, and contract renewal decisions, preventing the analysis from being reduced to a merely formal step.

- ☐ The due diligence policy expressly recognizes its own limits and provides for responses to situations where signs of illicit links arise, even after formal compliance with procedures.
- ☐ Partners, directors, attorneys-in-fact, intermediaries, and representatives are mapped, and addresses, bank accounts, telephone numbers, and shared links are identified.
- ☐ Data from suppliers, sub-suppliers, and service providers are cross-referenced, applying network analytics techniques to reveal hidden networks.

---

3. Traceability and Documentation

- ☐ The company ensures traceability of what was done, by whom, and for what reason, through minimal and standardized documentation regarding contracts, amendments, measurements, payments, and approvals.
- ☐ Critical fields are standardized, such as: CNPJ (National Registry of Legal Entities) or ultimate beneficial owner identification, destination bank account, cost center, base contract, reason for hiring, and the person responsible for approval.
- ☐ The following are consistently included in the records: contract, amendment or operational justification, supplier and CNPJ, destination bank details, linked cost center or project, requester, approver, rationale for the decision, and any exceptions.
- ☐ The company avoids verbal or informal approvals, records decisions in official channels, and fully documents exceptions.
- ☐ Clear rules exist for exceptions, including recording, justification, and appropriate oversight.

---

4. Red Flags and Warning Signs

- ☐ The company has created and maintains a red flag library that consolidates warning signs identified in internal processes.
- ☐ For each red flag, the library indicates the source process, severity level, and expected conduct.
- ☐ The following signs, among others, are monitored: unidentified ultimate beneficial owner, corporate changes without justification, operations incompatible with declared capacity, atypical use of logistical routes, urgent requests without adequate documentation, split payments, improper approaches to employees in critical roles, and interactions with recognized sensitive regions or sectors.
- ☐ The company remains vigilant for signs such as: frequent changes in bank accounts, prices incompatible with the market, intermediaries without a clear function, pressure for exceptions, discrepancies between contracted and executed services, and the recurring presence of unregistered third parties at the operational site.
- ☐ There is a clear workflow for handling warning signs, covering the stages of detection, qualification, recording, decision-making, and remediation, with defined responsibilities and escalation criteria proportional to the identified risk.

5. Incident Management and Decision Making

- ☐ There is a continuous cycle of detection, recording, and preservation of evidence, with systematic incorporation of lessons learned over time.
- ☐ There is a structured integration workflow between compliance, legal, human resources, operations, and other relevant areas, with defined responsibilities and orderly information sharing.
- ☐ Information is qualified, distinguishing between verifiable information (documents, system data), preliminary reports (requiring plausibility checks), and subjective perceptions (recorded for enhanced monitoring).
- ☐ Records and evidence are stored in a secure and traceable manner, with restricted access, recording of the chain of custody, and retention periods compatible with the complexity of the cases.
- ☐ Internal assessment and escalation distinguish between verifiable facts, objective evidence, and analytical hypotheses, reducing the risk of decision-making paralysis and avoiding rushed responses.
- ☐ Prioritization and escalation are considered in an integrated manner, considering potential severity (legal, regulatory, financial, reputational, and operational impacts) and urgency (time available to act before the risk worsens).
- ☐ There is immediate escalation for situations such as: signs of coercion, extortion, or threats to employees; signs of infiltration into critical processes; attempts to conceal or destroy information; explicit pressure for hiring or payments outside the regular workflow; suspicious changes to bank beneficiaries; and significant exposure to transnational crimes.
- ☐ Initial measures prioritize precautionary and reversible responses, such as temporary suspension of payments, expansion of due diligence, restriction of access to systems and facilities, and review of critical routes or suppliers.
- ☐ Decisions are documented, recording the elements considered, alternatives evaluated, and justifications adopted.

---

6. Internal Reporting Channels

- ☐ The company has widely publicized reporting channels, using clear and accessible language, which can be used by employees, directors, service providers, and other third parties in the supply chain.
- ☐ Transparent internal procedures have been established for the receipt, screening, investigation, and closure of reports.
- ☐ Explicit non-retaliation policies have been adopted, accompanied by monitoring and accountability mechanisms to identify and sanction retaliatory practices, including indirect or veiled ones.
- ☐ The whistleblower's identity is preserved whenever technically possible, using tools that allow for anonymity or, at the very least, confidential treatment, with access restricted to the professionals responsible for the investigation.
- ☐ There are clear criteria for the internal and external sharing of reported information, especially when communication with authorities is required.
- ☐ The company provides feedback on the status of the reports received.

7. Reporting to Competent Authorities

- ☐ Reporting to competent authorities must be carried out following a careful legal assessment aligned with the company's integrity strategy.
- ☐ External reporting observes criteria of necessity, adequacy, and proportionality, avoiding undue exposure that compromises the legal certainty of the company or its employees.
- ☐ The company ensures that there is minimal internal investigation and sufficient informational backing before reporting, avoiding premature communications.

---

8. Training and Organizational Culture

- ☐ The most exposed areas receive specific training: procurement, logistics, construction and services, commercial area and channels, finance and treasury, asset security, legal, compliance, and local leadership.
- ☐ Training content covers business-relevant typologies, red flags throughout processes, application of the exception policy, minimal record-keeping requirements, and escalation criteria.
- ☐ Internal communication translates concepts into operational reality, with recurring dilemmas such as "urgency," "referred supplier," and "bank account change."
- ☐ Microlearning practices are used, with short modules distributed throughout the year to increase retention and immediate application.
- ☐ Scenario-based training is conducted, with simulations and role-plays, including situations such as pressure to hire a "referred" supplier, out-of-flow urgencies, undue external interference, and attempts to obtain sensitive data.
- ☐ Leadership consistently reinforces the importance of controls, transparency, and recording (tone from the top).
- ☐ Safe spaces for dialogue and questioning are ensured, reducing blind spots and broadening early detection.
- ☐ The company adopts the speak-up by design logic, normalizing reports, questions, and requests for help as expected behavior.

9. Culture Indicators and Monitoring

- ☐ Culture indicators (KPIs and KRIs) are monitored, such as report volume and quality, recurrence by area, concentration of exceptions, waiver rates, and the percentage of trained critical third parties.
- ☐ These indicators are used to measure maturity, identify blind spots, and prioritize actions.
- ☐ Monitoring is understood as an imperfect and evolutionary process, integrated into governance, rather than an absolute guarantee against illicit risks.

---

10. Protection Measures and Business Continuity

- ☐ Security protocols guide the actions of employees exposed to higher-risk regions, routes, or counterparties, with guidelines for discreet conduct and, when necessary, covert action.
- ☐ Depending on the severity, temporary removal of threatened employees or those involved in sensitive situations is provided for.
- ☐ The company maps and activates alternative supply and logistics routes in environments with the presence of criminal groups.
- ☐ Third parties associated with consistent signs of irregularity are replaced temporarily or permanently, based on objective criteria of severity and materiality.
- ☐ For critical processes, contingency plans exist providing for minimum service levels, degraded operation, and previously tested parallel routes.
- ☐ Periodic review of geographical, sectoral, and behavioral risks is integrated into planning.
- ☐ Internal and external communication is conducted in a careful, coordinated, and consistent manner, avoiding the informal circulation of sensitive information.
- ☐ Loss limits, escalation triggers, and criteria for the suspension, reduction, or relocation of operations are defined and reviewed in light of lessons learned.
- ☐ Assessment of indirect and collateral effects is continuous and multidisciplinary, incorporating compliance, operations, security, and procurement perspectives.

11. International Sanctions (for companies with a degree of internationalization)

- ☐ The company assesses its exposure to international sanctions, participation of US persons, dollar payments, use of US-origin technologies or services, and global supply chains.
- ☐ Proportional controls aligned with recognized references are adopted, such as OFAC and its framework for sanctions programs, as well as public risk guidelines.

---

12. Continuous Review and Institutional Learning

- ☐ Prevention, detection, and response strategies are reviewed continuously as new patterns of action and vulnerabilities become evident.
- ☐ The company promotes a preventive culture, post-incident learning, update of the red flag library, and continuous improvement of workflows.
- ☐ The effectiveness of measures depends on the integration of governance, compliance, operations, and organizational culture, with continuous review of mechanisms in the face of constant adaptation by criminal organizations.


ICC
Brasil

International Chamber of Commerce - Brazil (ICC Brasil)
Rua Surubim, 504 – 12th floor
Brooklin – São Paulo – SP – Zip Code 04571-050, Brazil
www.iccbrasil.org