

CODE OF ETHICS
AND INTEGRITY

CORPORATE
IMPLEMENTATION GUIDE



CONTENTS

1. Fundamentals of the Code of Ethics and Integrity	2	<ul style="list-style-type: none"> Why is it essential to the company's success? (p. 2) Scope and Application (p. 3) Strategic objectives of the Code (p. 4) Specific advantages by type of company (p. 5)
2. Key Components and Structure	6	
3. Step-by-Step Implementation Guide	20	
4. Timing and Continuous Adaptation	23	<ul style="list-style-type: none"> Preparation phase (p. 20) Design phase (p. 21) Validation and approval phase (p. 21) Implementation and training phase (p. 22) Monitoring and continuous improvement phase (p. 22)
5. Implementation Challenges and Critical Scenarios	25	
6. Annexes and Resources	27	
Glossary of Terms	27	
Annex I: Ethics in Cybersecurity	28	
Annex II: Digital Ethics and Responsible AI	30	
Annex III: Behavioral Ethics and the Importance of "Social Norms"	32	
Annex IV: Key performance Indicators (KPIs) for Codes of Ethics and Integrity	35	
Annex V: Example of Ethical Risk Matrix	37	
Annex VI: Ethical Case Investigation Template	40	

About the Authors | Cefeidas Group

Cefeidas Group is an international advisory firm that helps clients achieve their goals in Latin America. Cefeidas has worked with IDB Invest and the IDB for over a decade. Cefeidas provides professional services in public policy, risk and strategy; corporate governance, stewardship and sustainability; and strategic intelligence and research. www.cefeidas.com



1. FUNDAMENTALS OF THE CODE OF ETHICS AND INTEGRITY

A **Code of Ethics and Integrity** is the fundamental document that establishes the principles, values and guidelines of conduct that should govern the behavior of all members of an organization. It is the company's moral compass that articulates expectations about how employees, managers and directors should act in the performance of their functions and in their relationship with stakeholders.

This document goes further than solely legal compliance to become a fundamental strategic tool. It is the formal expression of organizational culture and represents the organization's commitment to higher ethical standards that guide daily decision-making and strengthen corporate reputation.

A well-designed Code should be:

- **Clear and understandable:** Written in plain language that everyone can understand.
- **Comprehensive:** That covers the main areas of ethical risk of the company.
- **Practical:** With examples and real situations that facilitate their application.
- **Current:** Subject to periodic reviews to maintain relevance.

Why is it essential to the company's success?

In today's business environment, characterized by increased public scrutiny, stricter regulations, and high *stakeholder* expectations, having a robust Code of Ethics has become a strategic necessity that directly impacts three critical dimensions:

Business Sustainability: A well-implemented Code builds lasting trust with clients who prefer to do business with whole companies, employees who develop pride in belonging, and communities that grant the social license to operate. Companies with strong ethical cultures demonstrate superior organizational resilience, with greater ability to overcome reputational crises, adapt to regulatory changes, and maintain operational continuity in adverse contexts.

Comprehensive risk management: The Code functions as an early warning and prevention system. In the legal and regulatory field, it prevents penalties and fines while reducing the incidence of litigation. Reputational risks, which can destroy in days the value built up over decades, are managed through systematic protection against scandals. From an operational perspective, the Code establishes effective barriers against internal fraud,

Practical note:

An effective Code of Ethics is not based on how many pages it has or how many topics it covers, but rather is one that is actually put into practice within the organization. The key is in the implementation and its ability to influence everyday decisions.

Code of Ethics vs. Code of Conduct: What's the difference?

Although these terms are used interchangeably, there is an important conceptual distinction:

Code of Ethics: Focuses on the core principles and values that guide behavior. It is more aspirational and philosophical, defining "why" we act a certain way and what the organization stands for. It addresses complex moral dilemmas and establishes the ethical framework for decision-making.

Code of Conduct: Focuses on specific expected rules and behaviors. It is more prescriptive and operational, defining "what" can and cannot be done in specific situations. Set clear behavioral standards with practical examples.

In practice, the most effective documents integrate both approaches. This guide adopts the term "Code of Ethics and Integrity" to emphasize both moral principles and expected behaviors.

undeclared conflicts of interest and vulnerabilities in the supply chain.

Value creation and access to capital: Business ethics is a tangible cause of good organizational performance. Companies with effective and well-implemented codes of ethics typically experience substantial improvements in key indicators: reduction in staff turnover, increases in productivity, and improvements in the work environment. These operational benefits translate into concrete financial advantages, including greater access to preferential rate financing, eligibility for ESG (*Environmental, Social, and Governance*) funds that are increasingly relevant in capital markets, and higher valuations in merger and acquisition transactions. While specific outcomes vary by sector, size, and context of each organization, the correlation between robust integrity programs and improved business performance is amply documented in the corporate governance literature.

Universal reach and application

The Code of Ethics and Integrity must have a **universal scope** within the organization and extend to its value chain. It should specifically apply to:

- **Corporate governance:** The Board of Directors, Board committees (particularly the Audit and Risk), and independent directors, who establish the "tone from the top".
- **Executive and operational structure:** The CEO and Senior Management, middle managers, who transmit the values in the daily operation, all employees regardless of their hierarchical level or type of contract, and temporary staff including consultants and interns.
- **Extended value chain:** Suppliers and contractors who must adhere to compatible ethical standards, business partners in joint ventures and strategic alliances, and intermediaries such as agents and distributors acting on behalf of the company.

Note: Regardless of the name your organization chooses, the fundamental thing is that the document is comprehensive, practical and put into practice in the daily organizational culture.

Success indicators

Organizations that effectively implement their Codes of Ethics report significant improvements in operational and organizational culture metrics, including noticeable reduction in ethical incidents, lower staff turnover, and better work environment.



Alert!

The lack of universal application of the Code creates "grey areas" where unethical behavior can proliferate. **IDB Invest** considers it essential that the Code applies to EVERYONE without exception.



Disclosure as a Pillar of Credibility

An undisclosed Code of Ethics limits its effectiveness. Transparency towards all *stakeholders* not only demonstrates a genuine commitment to integrity, but also strengthens trust and accountability. A poorly implemented code is a missed opportunity to build reputation, knowledge, and adherence.

Strategic Objectives of the Code

The Code pursues concrete objectives that go beyond declarations of good intentions:

Establish the ethical framework for action by defining clear boundaries between the acceptable and the unacceptable, providing criteria for ethical decision-making and establishing the basis for a culture of sustainable integrity. In terms of innovation, an environment of ethical trust fosters the proposition of new ideas, improves interdepartmental collaboration and generates greater openness to organizational change.

Protect the organization and its stakeholders by proactively mitigating legal, regulatory and reputational risks, preventing conduct that may harm the company, and safeguarding the interests of shareholders, employees and third parties. Operational risks find in the Code of Ethics an effective barrier against internal fraud, undeclared conflicts of interest and vulnerabilities in the supply chain.

Strengthen competitiveness by facilitating access to international markets that demand compliance with global standards, satisfying due diligence requirements of sophisticated institutional investors, and creating sustainable differentiation in markets increasingly aware of the importance of business integrity.



Corruption Perceptions Index (CPI)

Transparency International annually publishes the CPI index that ranks countries “by their perceived levels of corruption in the public sector,” and is determined by opinion polls and expert assessments. If only countries in the G20 are taken into account, Latin America and the Caribbean has three countries in the top 5 of the most corrupt:

1. Russia (CPI 154)

2. Mexico (CPI 140)

3. Brazil (CPI 107)

4. Turkey (CPI 107)

5. Argentina (CPI 99)

Source: [Corruption Perception Index 2024, Transparency International](#)

Link to the pillars of good corporate governance

The Code of Ethics is one of the cornerstones of good corporate governance, bringing its fundamental principles recognized by the Organisation for Economic Co-operation and Development (OECD) to reality. As the IBGC Code of Best Practices of Corporate Governance (6th edition) points out, “*ethics are the set of values and principles that guide conduct and enable the coexistence and evolution of human beings in increasingly complex societies. It is the foundation of the five principles of corporate governance: integrity, transparency, equity, accountability and sustainability.*”

- **Accountability** is realized through clearly defined responsibilities, robust reporting mechanisms, and consequence systems that ensure compliance.
- **Fairness** ensures fair treatment of all stakeholders and ensures equal opportunities.
- **Responsibility** clarifies fiduciary duties and sets high standards of professional care.
- **Transparency** promotes the proper disclosure of information and builds trust through responsible openness.

Specific Benefits by Type of Company

Family Businesses

For family businesses, the Code of Ethics represents a fundamental professionalization tool that makes it possible to effectively separate the family and business spheres. It facilitates orderly generational transitions by establishing clear rules that transcend personal relationships, reduces over-dependence on founders by institutionalizing processes, and preserves positive family values by formalizing them in company culture.

SMEs

Within the Code of Ethics, small and medium-sized enterprises find a structure that facilitates their orderly and scalable growth. It becomes a requirement frequently demanded by corporate clients looking for reliable suppliers, prepares the company for investment processes where integrity is fundamental in *due diligence* processes and generates a clear differentiation from competitors that operate informally.

Listed Companies

For publicly traded companies, the Code of Ethics transcends good practice to become a mandatory regulatory requirement in many securities markets. It is a central element in analysts' and investors' assessment of corporate governance, directly impacts the share price, and provides protection against shareholder activism that challenges corporate practices.

Multinationals

Multinational corporations face the challenge of maintaining global coherence in their ethical standards while respecting local particularities. The Code provides a unified framework for managing the complexity of operating across multiple jurisdictions, protects the global brand against reputational risks that can arise in any geography, and enables integrity standards to be extended across the global supply chain.

References to international standards

The **OECD Principles of Corporate Governance** clearly state that the Board of Directors must apply high ethical standards and has the primary responsibility for setting the "ethical tone" of the company. These principles recognize codes of conduct as fundamental tools for ensuring corporate integrity and state that they must be an integral part of the corporate governance framework.

Other voluntary standards such as **the UN Global Compact or the OECD Guidelines for Multinational Enterprises** on Responsible Business Conduct strongly integrate ethics by recommending that companies apply due diligence to identify, prevent and mitigate adverse impacts on human rights, labor rights, the environment and other areas.

There are also voluntary international standards developed by experts to establish quality standards such as **ISO 37001 for anti-bribery management systems, ISO 37301 for compliance management systems** in which the company can be certified.

Regulations such as **the US Foreign Corrupt Practices Act (FCPA) and the UK Bribery Act** have become not only reference frameworks but increasingly requirements to access certain markets or types of financing.

2. KEY COMPONENTS AND STRUCTURE

Breakdown of Essential Elements

The following is a simple template for drafting the code. Companies are encouraged to develop their own detailed documents:

Cover Page

CODE OF ETHICS AND CONDUCT

[Company name]

Contents:

I. INTRODUCTION

A. Leadership Message

B. Our History and Values

C. How to Use this Code

II. BASIC ELEMENTS

A. Purpose of the Code

B. Who the Code Applies to

C. Individual Responsibilities

D. Leader Responsibilities

III. OUR COMMITMENTS

A. With Our Employees

1. Respectful Work Environment

2. Diversity and Inclusion

3. Health and Safety

B. With Our Clients

1. Quality and Service

2. Honest Marketing

3. Data Privacy

C. With Our Shareholders

1. Accurate Financial Information

2. Protection of Assets

3. Conflicts of Interest

D. With Society

1. Environmental Responsibility

2. Community Participation

Don't forget to include:

- Date approved by the Board
- Validity and next revision.
- Document custodian.
- Document version.
- The index should be comprehensive to facilitate quick navigation.

3. Human rights

IV. BUSINESS INTEGRITY

A. Anti-Corruption and Bribery

B. Gifts and Entertainment

C. Political Contributions

D. Fair Competition

E. International Trade

F. Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT)

V. HANDLING INFORMATION

A. Confidentiality

B. External Communication

C. Social Media

D. Records and Documentation

VI. COMPLIANCE AND CONSEQUENCES

A. Reporting Channels

B. Investigation Process

C. Disciplinary Measures

D. Non-Retaliation

E. Monitoring Structure

F. Investigation Process

VII. RESOURCES AND CONTACTS

A. FAQs

B. Key Contacts

C. Related Policies

D. Certification Form

I. INTRODUCTION

A. Leadership Message

Dear employees:

At *[Company Name]*, integrity is non-negotiable. It is the foundation on which we build our business, develop lasting relationships and create sustainable value for all our stakeholders.

Maximum length of 1-2 pages. It should be a joint statement from the Chairman of the Board and the CEO that unequivocally sets out the commitment to business ethics. It should not be an empty formality but a personal and direct statement communicating the vital importance of integrity for sustainable success. The tone should be serious but personal, direct and inspiring.

This Code of Ethics and Integrity reflects our core values and sets out the behavioral expectations for all of us, without exception. It's not simply a compliance document; it's a practical guide to day-to-day decision-making that helps us maintain the highest ethical standards in everything we do.

Each of us has a personal responsibility to know, understand and implement this Code. We ask that you read it carefully, participate in trainings, and don't hesitate to ask questions when faced with ambiguous situations.

We want to be absolutely clear: we will not tolerate violations of this Code, no matter who commits them or the circumstances. At the same time, we guarantee full protection against retaliation for those who report concerns in good faith.

Together, we will maintain [Company Name]'s reputation as an organization that can be trusted.

[Signature]

[Signature]

[Name] - Chairman of the Board

[Name] - CEO

B. Our History and Values

[Complete with company history]

Our decisions and actions are guided by these core values:

INTEGRITY: We act with honesty, transparency and consistency between what we say and what we do.

RESPECT: We value the dignity, diversity and rights of all people.

RESPONSIBILITY: We assume the consequences of our decisions and actions.

EXCELLENCE: We are constantly looking to improve and exceed expectations.

COLLABORATION: We work together to achieve common goals.

[Other]

C. How to Use this Code

[To complete - Explain the structure of the document, how to find specific information, and when to refer to each section. Include references and visualizations to support tools and additional resources available].

Some key elements to be included:

Personal connection to values, recognition of real ethical challenges, unequivocal commitment to integrity, clear expectation of universal compliance regardless of hierarchical level or geographic location, and assurance of protection from retaliation.

Avoid:

Generic corporate language, empty promises, or abstract statements with no connection to business reality.

Connection to corporate identity:

This section should connect the history of the company with its current values, showing the evolution and consistency of ethical commitment. Include relevant milestones that demonstrate the historical importance of integrity in the

II. BASIC ELEMENTS

A. Purpose of the Code

This Code of Ethics and Integrity sets out the principles and standards of behavior that guide our actions and decisions. Its goal is to:

- *Protect our reputation and the trust we have built with our stakeholders.*
- *Provide clear guidance for ethical decision-making in complex or ambiguous situations.*
- *Ensure compliance with all applicable laws and regulations in the countries where we operate.*
- *Strengthen our culture of integrity and transparency.*

- *Create sustainable value for shareholders, employees, clients and society.*
- *[Other]*

B. Who the Code Applies to

This Code mandatorily applies to all persons acting on behalf of [Company Name], including:

- *Members of the Board.*
- *All employees, regardless of geographic location, type of contract, or hierarchical level.*
- *Consultants, contractors, interns and temporary staff working on our premises or on our behalf.*
- *Agents, intermediaries, distributors and business partners when acting on behalf of the company.*

We expect our suppliers, clients, and business partners to share these principles and maintain ethical standards consistent with ours.

C. Individual Responsibilities

All employees are responsible for:

- *Knowing, understanding and complying with this Code and related policies.*
- *Seeking guidance when in doubt about the application of the Code.*
- *Completing all required ethics and compliance training in a timely manner.*
- *Immediately reporting any known or suspected violations.*
- *Fully cooperating in internal investigations.*
- *Certifying annually their understanding of and compliance with the Code.*

D. Leader Responsibilities

Leaders and supervisors have additional responsibilities:

- *Model exemplary ethical behavior in all their actions.*
- *Ensure your team knows and understands the Code.*

Articulation of the “why”:

The purpose section should go beyond generic statements about “doing the right thing” to make concrete connections between ethical behavior and business success. It should explain how the Code protects the company, its employees and *stakeholders*, facilitates decision-making in ambiguous situations and strengthens corporate reputation as a key strategic asset.

Specific and measurable objectives:

Each objective must be connected with a tangible benefit for the organization and its stakeholders.

This section should precisely define to whom the Code applies, avoiding ambiguities that may create “grey zones” of non-compliance. It should specify its universal application at all organizational levels and include clear expectations for third parties. The wording must contemplate special situations such as mergers, acquisitions and joint ventures if necessary.

The “tone from above”

Leaders should be the first and best examples of expected behavior. Leaders have increased responsibilities that reflect their role in creating and maintaining ethical culture.

- Create a safe environment where employees feel comfortable asking questions and reporting concerns.
- Appropriately raise ethical concerns that they receive.
- Never retaliate or tolerate retaliation.
- Apply consequences fairly and consistently, without favoritism.

III. OUR COMMITMENTS

A. With Our Employees

1. Respectful Work Environment

We are committed to maintaining a work environment where all people are treated with dignity and respect. We do not tolerate any form of discrimination based on: race, color, ethnic origin or nationality, gender or gender expression, sexual orientation or gender identity, religion or belief, age, disability, marital or family status, socioeconomic status, political opinions, or any other characteristic protected by law.

We do not tolerate any form of harassment, including: sexual harassment (unwanted advances, requests for sexual favors, verbal or physical conduct of a sexual nature), psychological harassment (intimidation, humiliation, threats, bullying), physical or verbal violence, cyberbullying, or misuse of digital media to harass or intimidate.

2. Diversity and Inclusion

We value diversity of perspectives, experiences, and talents. We actively promote inclusion and equal opportunities for all.

3. Health and Safety

The safety and health of our employees is a top priority. Everyone must comply with safety regulations and report unsafe conditions immediately.

B. With Our Clients

1. Quality and Service

We are committed to providing the highest quality products and services and meeting or exceeding our clients' expectations.

2. Honest Marketing

All our marketing and advertising communications must be truthful, accurate and not misleading. Avoid exaggerations or promises that cannot be kept.

3. Data Privacy

We respect and protect the privacy and personal data of our clients, complying with all applicable data protection laws.

[Refer to Data Privacy Policy, if any].

Commitment to human capital:

This section sets out the company's commitment to creating and maintaining a decent, safe and respectful work environment.

Inclusive and updated list:

The list should cover all categories protected by local and international legislation and be updated regularly to reflect social and legal developments.

Clear definitions of prohibited conduct:

It is crucial to provide specific examples to avoid ambiguity about what constitutes harassment. For example, the inclusion of cyberbullying reflects the reality of modern work environments.



Ethics in Cybersecurity

Ethical cybersecurity involves not only technical controls, but also clear principles on responsible use of systems, data protection and transparency in incidents, extending the concepts of confidentiality, integrity and availability to moral responsibilities with all stakeholders. For further guidance on its governance and integration with the Code of Ethics, see [Annex I](#).

C. With Our Shareholders

1. Accurate Financial Information

We maintain accurate and complete financial records. All financial information must faithfully reflect the reality of our operations.

2. Protection of Assets

Company assets (physical, financial, intellectual and digital) must be used exclusively for legitimate business purposes and protected against loss, damage or misuse.

3. Conflicts of Interest

A conflict of interest arises when personal interests interfere or could interfere with the ability to make objective decisions for the benefit of the company.

Common situations that can lead to conflict:

- Familial or personal relationships with suppliers, clients or competitors.
- Significant financial investments in companies related to our business.
- External activities that compete with the company's time or resources.
- Business opportunities that arise from the position in the company.

Conflict Management Process:

1. IDENTIFY: Recognize when a conflict exists or could exist.
2. DECLARE: Immediately inform the supervisor and the Compliance Officer.
3. REFRAIN: Do not participate in related decisions until guidance is received.
4. DOCUMENT: Record the conflict and its resolution in the appropriate systems.

[Refer to Conflicts of Interest Policy, if any].

D. With Society

1. Environmental Responsibility

We are committed to minimizing our environmental impact and promoting sustainability across our operations.

[Connect with specific, measurable goals when possible].

2. Community Engagement

We contribute positively to the communities where we operate through social investment, volunteering and collaboration with local organizations.



Ethics and Artificial Intelligence

The use of digital technologies and AI raises ethical dilemmas about bias, transparency and accountability in the use of company assets, so organizations must define principles of algorithmic transparency, equity and human oversight, especially in the context of Latin America and the Caribbean (see Annex II).

Clear and documented steps:

The process should be simple and non-punitive to encourage pro-active declaration.



Ethics and Climate Governance

Climate governance requires integrating climate change risks and opportunities into the business ethical framework, considering environmental impacts, resilience and low-carbon transition, in line with international standards and with particular relevance for Latin America and the Caribbean.

3. Human Rights

We respect and promote fundamental human rights throughout our operations and supply chain.

IV. BUSINESS INTEGRITY

A. Anti-Corruption and Bribery

We have zero tolerance for any form of corruption or bribery. Strictly prohibited are:

- Offering, promising, giving or authorizing payments, gifts or anything of value to public or private officials to obtain or retain undue advantages.
- Soliciting or accepting bribes, kickbacks, or improper payments of any kind.
- Making facilitation payments, regardless of the amount or circumstances.
- Using third parties to perform acts that we cannot do directly.

Practical example: A provider suggests that they can “expedite” obtaining a government permit in exchange for an unofficial extra payment. Correct answer: Immediately reject the proposal and report the incident to the Compliance Officer.

[Refer to the Anti-Corruption Policy, if any].

B. Gifts and Entertainment

Business gifts and entertainment can create real or perceived conflicts of interest.

We can ACCEPT:

- Promotional items of nominal value (less than \$[XX] USD or local equivalent).
- Occasional and reasonable business meals.
- Invitations to events where our participation has a legitimate business purpose.

We must NEVER:

- Accept cash or cash equivalents (gift cards, loans, stocks).
- Solicit gifts or personal favors of any kind.
- Accept gifts during bidding, negotiation or audit processes.

We must CONSULT before accepting:

- Any gift with a value greater than \$[XX]USD.
- Trips paid for by third parties.
- Entertainment that could be perceived as luxurious or excessive.

Practical example: A supplier with whom you are negotiating an important contract invites you to a weekend of golf at a luxury resort, with all expenses paid, as a “thank you for the business relationship.” Correct answer: Politely decline the invitation, explain that company policies do not allow accepting hospitality of this type during active

Specificity and Relevance:

The document should reflect the ethical risks specific to the company's industry, geography and business model. For example, a pharmaceutical company will emphasize integrity in clinical research, while a financial institution will focus on the prevention of money laundering.

Real cases to clarify:

Concrete examples help employees recognize risky situations in their daily work.

negotiations, and report the offer to the Compliance Officer for registration.

[Establish who to consult and the approval process. Refer to the Gifts and Entertainment Policy, if any].

C. Political Contributions

The company does not make contributions to political parties or candidates. Employees may engage in political activities in their personal capacity, outside of working hours, and without using company resources.

D. Fair Competition

We compete vigorously, but fairly and honestly. It is prohibited to: engage in anti-competitive practices, obtain information from competitors by inappropriate means, or make false statements about competitors.

[Include references to relevant antitrust laws].

E. International Trade

We comply with all applicable international trade laws, including export/import regulations, economic sanctions, and anti-money laundering laws.

F. Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT)

We are committed to preventing our products, services and operations from being used for money laundering or terrorist financing.

Employees are expected to:

- Know and comply with all applicable AML/CFT policies and procedures.
- Verify the identity of clients and counterparties according to established procedures (KYC - Know Your Client).
- Immediately report any suspicious or unusual transactions to the Compliance Officer.
- Never alert the customer about suspicious transaction reports (STRs).
- Maintain complete and accurate records of all transactions as per regulatory requirements.

Warning signs that require special attention:

- Clients who avoid providing complete or verifiable information.
- Transactions with no apparent economic purpose or inconsistent with the customer's profile.
- Structuring of transactions to avoid reporting thresholds.
- Unusual requests for confidentiality or unconventional payment methods.
- Transactions with high-risk jurisdictions or politically exposed persons (PEPs).
- *[Adapt examples to regional context and type of business].*

Corporate political neutrality:

Clarify the distinction between corporate and personal activities. Adjust according to local legislation on political financing.

Failure to comply with AML/CFT regulations can result in severe consequences for both the company and the individuals involved, including criminal penalties.

V. HANDLING INFORMATION

A. Confidentiality

We must protect all confidential information of the company, clients and partners. Confidential information includes: business strategies and plans, non-public financial data, technical information and know-how, personal data of employees and clients, terms of contracts and agreements, information on potential mergers or acquisitions.

This obligation of confidentiality continues even after the termination of the employment relationship with the company for a period of [X] years.

[Refer to the Information Security Policy, if any].

B. External Communication

Only authorized spokespersons may make public statements on behalf of the company. Employees should direct all media inquiries to the Communications department.

[Refer to the Communication Policy, if any].

C. Social Media

When using social media, employees should: clearly distinguish between personal opinions and company positions, not disclose confidential information, be respectful and professional, remember that their posts may affect the company's reputation.

D. Records and Documentation

All company records must be accurate, complete, and faithfully reflect the transactions they document. It is forbidden to falsify documents, conceal or destroy records subject to investigation or legal withholding.

VI. COMPLIANCE AND CONSEQUENCES

A. Reporting Channels

If you observe or suspect a violation of this Code, you have an obligation to report it. This can be done through:

- *Your direct supervisor or any member of management.*
- *The Human Resources department.*
- *The Compliance Officer.*
- *The Ethics Line (available 24/7):*
 - *Phone: [Toll Free 0800-XXX-XXXX] (toll free)*
 - *Website: [Link to website]*
 - *Email: [Link to email]*
 - *Physical mailbox located at [location]*

Clear Classification"

Assist employees in identifying what information requires special protection.



External Experts

The company can fall into the trap of relying excessively on external consultants or generic best practices without sufficient internal adaptation. While external knowledge is valuable, organizations that completely outsource the development of their Code end up with technically correct but culturally alien documents.

Organizations must cultivate a culture that sees ethical mistakes as learning opportunities, not merely as offenses to be punished. This does not mean tolerating serious violations, but creating safe spaces to discuss dilemmas, admit minor mistakes, and learn collectively. This requires a good ethical culture.

We guarantee:

- Absolute confidentiality in the handling of all complaints.
- An option to make anonymous reports when preferred.
- Fair, objective and timely investigation of all allegations.
- Full protection against any form of retaliation.

B. Investigation Process

All complaints will be investigated following these principles: confidentiality (protection of the identity of the complainant and those involved), objectivity (impartial investigation without prejudice), timeliness (resolution within reasonable deadlines), documentation (appropriate recording of the entire process), proportionality (adequate response to the gravity of the fault).

[The Code should clearly state the whistleblower investigation process, including accountability, timelines, and due process guarantees (tailored to your company's resources and needs). Consequences for violations must be explicitly defined, from corrective measures to termination of employment, consistently applicable regardless of the hierarchical level of the offender].

Below is the general research flow:

[Stage 1: Reception and Initial Evaluation (1-3 business days)

Responsible: Compliance Officer

Activities: Registration of the case, preliminary assessment of the severity, determination of whether a formal investigation is appropriate, and assignment of priority level.

Stage 2: Assignment and Planning (2-5 business days)

Responsible: Compliance Officer/Ethics Committee

Activities: Designation of the investigation team [which may include Legal, Human Resources, Internal Audit, or external advisors according to complexity], definition of the scope of the investigation, and preparation of the work plan.

Stage 3: Field Research (typically 15-30 business days)

Responsible: Research Team

Activities: Collection of documentary and digital evidence, confidential interviews with the complainant, respondent, witnesses and other relevant persons, analysis of the information collected, and detailed documentation of the process.

Stage 4: Analysis and Conclusions (5-10 business days)

Responsible: Research Team

Activities: Evaluation of findings against applicable policies and regulations, determination of whether or not there was a violation of the Code,

Preparation of the investigation report with recommendations, and presentation to the Compliance Officer.

Whistleblower Protection: Our Guarantee

A successful ethics program depends on employees feeling safe reporting concerns. For this reason, protection against retaliation is the company's top priority.

Active protection mechanisms:

- Continuous post-report monitoring
- Immediate investigation of retaliation
- Severe penalties with no exceptions
- Extended case follow-up

Reporting in good faith is an act of loyalty to the company and those who report deserve our maximum protection and recognition.

Indicative deadlines:

These deadlines may be justifiably extended in cases involving multiple jurisdictions, large volume of digital evidence, or need for specialized technical expertise. The Compliance Officer (or whoever is in charge of the process) will keep the whistleblower informed about the progress of the investigation, respecting the confidentiality limitations of the process.

Stage 5: Resolution and Measures (5-10 business days)

Responsible: Compliance Officer/Ethics Committee/Senior Management/Board of Directors

Activities: Review of the investigation report, determination of proportional disciplinary measures (if applicable), approval of systemic corrective measures (by the corresponding body according to the sanction), and communication of the resolution to the parties involved respecting confidentiality.

Stage 6: Follow-up (periodic in X weeks)

Responsible: Compliance Officer

Activities: Verification of implementation of corrective measures, monitoring of non-retaliation against the whistleblower, appropriate filing of documentation, and drawing lessons learned for future prevention].

C. Disciplinary Measures

Violations of this Code will result in disciplinary action commensurate with the severity of the offense, which may include: additional guidance or training (for minor or unintentional offenses), verbal or written reprimand, suspension with or without pay, demotion or reassignment of duties, termination of employment, legal action when the violation constitutes a crime.

Consequences will be applied consistently, regardless of the hierarchical level or position of the person involved.

D. Non-Retaliation

We strictly prohibit any form of retaliation against individuals who: report concerns in good faith, participate in investigations, refuse to engage in conduct that violates this Code.

Retaliation is considered a serious violation of this Code and will result in severe disciplinary action, including immediate termination of employment.

E. Monitoring Structure

1. Role of the Board of Directors

The Board of Directors has the following responsibilities regarding the Code:

- Approve the Code and its annual updates.
- Oversee the effective implementation of the ethics program.
- Receive and evaluate quarterly reports on: statistics of complaints received and resolved, trends and patterns identified, significant cases and their resolutions, effectiveness of corrective measures.
- Ensure adequate resources for the compliance program.
- Model expected ethical behavior across the organization.

Catalogue of Disciplinary Measures

To ensure consistency and transparency it is recommended to develop a formal catalogue of disciplinary measures with:

- **Type of offenses:** Classification by severity (minor, serious, very serious).
- **Range of Consequences:** From orientation to termination.
- **Proportionality criteria:** Aggravating and mitigating factors to consider.
- **Decision process:** Who determines the measure according to the level of severity.

The catalogue must be indicative, not exhaustive or limiting. Each case requires assessment of specific circumstances, allowing reasoned discretion to apply proportional and fair consequences.

Definition of Retaliation:

Include in the Code examples such as: unjustified negative changes in evaluations, exclusion from projects or meetings, hostility or isolation, direct or indirect threats.

Organizational proportionality:

The supervisory structure must be adapted to the size and resources of each company. Smaller organizations can concentrate multiple functions in fewer roles, always maintaining the essential features.

[These functions may also be reflected in the Regulations of the Board of Directors, if any].

2. Role of the Compliance Officer

The Compliance Officer is the executive responsible for the ethics program and reports directly to the CEO and Board. Their responsibilities are to:

- Manage the day-to-day of the ethics and compliance program.
- Coordinate the periodic updating of the Code.
- Oversee training and certification programs.
- Manage reporting channels and ensure their 24/7 operation.
- Coordinate impartial and timely investigations.
- Advise employees and management on complex ethical dilemmas.
- Maintain confidential records and program statistics.
- Prepare regular reports for Senior Management and the Board.

3. Ethics Committee

The Ethics Committee is composed of:

- The compliance officer, who chairs it.
- Director of Human Resources
- Legal Director.
- Head of Internal Audit.
- A rotating representative of the operational areas.
- At least one independent external member.

The Committee meets monthly and has the authority to:

- Evaluate and resolve complex ethical cases.
- Review trends and recommend preventive actions.
- Propose updates to policies and procedures.
- Approve justified exceptions to policies (documenting reasons).

[Refer to the Regulations of the Ethics Committee and the Complaints Handling Policy, if any].

4. Human Resources

Human Resources has specific responsibilities in:

- **Recruitment:** Evaluate candidate integrity through referrals and verifications.
- **Induction:** Ensure training on the Code in the first [XX] days.
- **Development:** Include ethics in all leadership and development programs.
- **Evaluation:** Incorporate ethical behavior as a criterion in performance evaluations.
- **Discipline:** Ensure consistent application of consequences for violations.
- **Exit:** Conduct exit interviews including questions about ethical culture.

5. Internal Audit

Internal Audit must:

Dual reporting to ensure independence:

Direct access to the Council is critical to avoid undue pressure.

- **Multidisciplinary composition** for diverse perspectives.
- Include an **independent member** to give objectivity (provides external perspective and reduces groupthink risk).
- **Avoid including the CEO** or owner to avoid pressures and influences that undermine objectivity in the work of the rest.

Differentiated Training Program

Training on the Code cannot be uniform across the organization. Different audiences require different approaches, depth, and examples:

- Board of Directors: executive session (2-3 hours).
- Senior Management: ethical leadership workshop (1 day).
- Middle Management: practical training (4-6 hours).
- General Employees: interactive training (2-3 hours).
- New Employees: induction

- Include evaluation of the ethics program in your annual audit plan.
- Evaluate the effectiveness of controls related to ethical risks.
- Test the operation of reporting channels (including anonymity tests).
- Review completed research to assess consistency and level of detail.
- Report findings directly to the Board Audit Committee.

6. Legal

The Legal department provides:

- Advice on legal implications of violations of the Code.
- Coordination with authorities when required.
- Updates on relevant regulatory changes.
- Support for sensitive or high-risk investigations.

VII. RESOURCES AND CONTACTS

A. FAQs

[Include section with questions and answers about common ethical situations in the company. Develop based on actual queries received. Update regularly with new cases and situations].

B. Key Contacts

- Compliance Officer: *[Name, Phone, Email]*
- Human Resources: *[Contact]*
- Legal Advice: *[Contact]*
- Ethics Line: *[Numbers and Means]*

C. Related Policies

This Code should be read in conjunction with the following specific policies: Anti-Corruption Policy, Conflicts of Interest Policy, Gifts and Entertainment Policy, Data Privacy Policy, Information Security Policy, Human Resources Manual, Communications Policy, Internal Work Regulations.

D. Certification Form

Annual certification

All employees must certify annually that: they have read and understood the Code in its entirety, they will comply with all its provisions, they have reported any known or suspected violation, they have declared all existing or potential conflicts of interest, they understand the consequences of non-compliance.

[Include model of the form or link to it].

Ethical Decision Test

When faced with a difficult decision, ask yourself:

Systemic Integration:

The Code should not exist in isolation but be fully integrated with other elements of the governance system: specific policies that delve into particular issues, training programs that translate principles into behaviors, performance management systems that recognize ethical conduct, and *due diligence* processes that extend the standards to third parties.

Certification and Commitment

Each employee must not only receive training but also formally certify that they have read, understood, and are committed to complying with the Code. This certification process, which must be repeated annually, serves multiple purposes: it reinforces the importance of the Code, provides legal protection to the organization, and creates a moment of personal reflection on ethical commitment.

The certification must also include the declaration of any existing or potential conflict of interest, creating a record as a baseline that can be updated periodically.

Is it legal? Is it consistent with our values and this Code? Would I feel comfortable if my decision was published in the media? Would it be a good example for others? Does it protect the company's reputation?

Validity and Updates

This Code was approved by the Board of Directors on [date].

It is reviewed annually and updated as necessary to reflect changes in applicable laws and regulations, business evolution and new risks identified, emerging best practices in business ethics, as well as lessons learned from incidents and ethical cases.

Last updated: [DATE]

Next scheduled review: [date]



Considerations for Effective Implementation

Excellence in design must be complemented by excellence in implementation. A masterfully drafted but poorly implemented Code is worse than not having a Code, as it generates cynicism and distrust.

Effective implementation requires:

- Ceremonial launch demonstrating leadership commitment.
- Training differentiated by levels and functions.
- Periodic certification that keeps the Code present.
- Continuous monitoring through ethical performance indicators.
- Constant communication about the importance of ethics.
- Recognition of exemplary ethical behaviors.
- Consistent application of consequences without exceptions.

The ultimate success of the Code is measured not by its literary elegance but by its **ability to influence the daily behavior of all members of the organization.**

The "Newspaper Test"

This cognitive ethical "nudge" triggers an aversion to public embarrassment and forces people to consider the external implications of their decisions. If the answer to any question is "No" or "Not sure," the employee should stop and seek guidance.



Behavioral **ethics** recognizes that biases and pressures can divert decisions, so organizations can apply ethical "nudges" as timely reminders, make positive behaviors visible and simplify reporting, facilitating correct choices without restricting freedom (see Annex III).



Indicator Framework

A model of indicators related to the Code of Ethics is presented in **Annex IV**. [Click here.](#)



Ethical Risk Matrix

An example of an Ethical Risk Matrix is presented in **Annex V**. [Click here.](#)



Research Template Model

A model Research Template is presented in **Annex VI**. [Click here.](#)

3. STEP-BY-STEP IMPLEMENTATION GUIDE

Successful implementation of a Code of Ethics requires a structured process that typically takes place in 9 to 12 months. It is essential to understand that implementation is not a single event but a process of cultural change that requires patience, persistence and adaptability. Organizations that approach this process as a mere regulatory formality invariably fail to capture the real benefits of a robust ethics program. On the contrary, those who see it as an opportunity to strengthen their culture and competitiveness find a powerful tool for organizational transformation in the Code.

Below, we present the five critical phases with their key actions:

Preparation Phase

1

Months 1 and 2

Objective: To establish the organizational bases and diagnose the current state of the ethical culture.

<p>Key Action 1 - Designate Leadership and Governance: Appoint a project leader with authority and direct access to the CEO and Board. Form a multidisciplinary Ethics Committee with representatives from key areas (Legal, HR, Operations, Finance).</p>	<p>Key Action 2 - Perform Comprehensive Diagnosis: Evaluate the current ethical culture through climate surveys, analysis of past incidents, and benchmarking with industry best practices. Identify specific ethical risks, taking into account the sector, geographical areas of operation and the value chain.</p>
---	--

The illusion of “set and done”
A dangerous trap is to treat the development and implementation of the Code as a project with an end date. Organizations that celebrate the launch of the Code as the end of the journey, rather than the beginning, are destined to see its effectiveness rapidly erode. On the other hand, paradoxically, the pursuit of perfection can become the enemy of effectiveness. Organizations that indefinitely postpone the release waiting for the “perfect” Code or delay the necessary updates for fear of admitting imperfections in the current version, miss valuable opportunities for incremental improvement.



Drafting Phase

2

Months 3 and 4

Objective: To develop the content of the Code based on the diagnosis and ensuring broad participation.

Key Action 3 - Define structure and content:

Based on the risks identified, establish the priority issues and the architecture of the document, balancing comprehensiveness with practical accessibility.

Key Action 4 - Participatory writing process:

Involve representatives from different areas and levels in the writing. Consult with external key *stakeholders* (clients, suppliers, investors) to incorporate their expectations.



The Frankenstein Code

A common mistake is to create a Code by copying and pasting from multiple sources without considering internal consistency or organizational relevance. This “*Frankenstein Code*” typically contains internal contradictions, uses inconsistent language, and addresses irrelevant issues while ignoring actual organizational risks.

For example, a financial services company that extensively copies industrial security policies from a manufacturing company, or a *startup* that adopts governance structures designed for multinational corporations. The result is a document that employees perceive as generic, irrelevant and disconnected from their daily reality.

Validation and Approval Phase

3

Months 5 and 6

Objective: To ensure legal soundness and obtain formal commitment at the highest level.

Key Action 5 - Legal review and coordination:

Verify compliance with legislation in all operating jurisdictions. Coordinate with existing policies and update those that require alignment.

Key Action 6 - Tiered approval:

Follow the formal process: review by the Ethics Committee, approval by Senior Management, validation by the Audit Committee, and final approval by the Board of Directors with complete documentation at each level.



Implementation and Training Phase

4

Months 7 and 8+

Objective: To launch the Code effectively and ensure its understanding and universal adoption.

Key Action 7 - Strategic launch:

Execute a multi-channel communication campaign led by the CEO and Chairman of the Board. Use various formats (videos, face-to-face/virtual sessions, printed materials) to maximize impact and recall.

Key Action 8 - Differentiated training program:

Implement audience-tailored training: executive session for the Board (2-3 hours), intensive workshop for Senior Management (1 day), hands-on training for middle managers (4-6 hours), and interactive modules for general employees (2-3 hours).

Key Action 9 - Certification and support systems:

Obtain formal certification from all employees confirming reading, comprehension and commitment. Activate 24/7 ethics hotline, resource portal and ethics ambassador network as consultation points.



Monitoring and Continuous Improvement Phase

5

Month 9 +

Objective: To ensure the sustained effectiveness of the Code through continuous evaluation and updating.

Key Action 10 - Comprehensive monitoring system:

Implement *dashboards* with quantitative (complaints, training, certifications) and qualitative (ethical climate, *stakeholder perceptions*) metrics.

Key Action 11 – Update:

Conduct formal annual review of the Code considering regulatory changes, new risks, lessons learned and business evolution.

Stalled or missing metrics

Organizations that do not systematically measure the effectiveness of their ethical program are navigating blindly. The absence of clear metrics, or worse, the collection of metrics that no one reviews or acts on, indicates a lack of real commitment to continuous improvement. Metrics that remain identical period after period suggest manipulation or irrelevance. See [Annex IV](#) to understand more about indicators.

4. TIMING AND CONTINUOUS ADAPTATION

The success of a Code of Ethics depends both on its content and on the time and manner in which it is implemented, reviewed and adapted. This chapter examines the critical temporal aspects and how to keep the Code relevant in changing contexts.



Critical Moments for Action

Organizations experience tipping points that create unique or imperative opportunities to strengthen their ethical framework. The **change in leadership**, particularly at the CEO or Chairman of the Board level, represents a natural opportunity to reinforce the organizational ethical tone. **Significant strategic transformations**, such as entering new markets or launching innovative lines of business, demand revision of the Code to ensure it addresses emerging ethical risks. **Mergers and acquisitions processes** require coordination of values and ethical standards between different organizational cultures, this being a critical moment where an updated Code can facilitate cultural integration. **Preparing for an initial public offering (IPO)** inevitably requires strengthening all aspects of governance, including the ethical framework.

In the external environment, **significant regulatory changes** require agile responses to incorporate new legal and ethical requirements. **Sectoral crises or scandals in comparable companies** serve as wake-up calls that should motivate preventive reviews. The **changing expectations of stakeholders**, particularly investors with ESG mandates and conscious consumers, create powerful imperatives for the continued evolution of the ethical framework.



Review and Update Cycles

International best practices converge in recommending a **formal annual review of the Code**, even if it does not result in substantial changes. This review should systematically examine changes in the regulatory environment, ethical incidents and lessons learned from them, evolution of best practices in the industry, and results of ethical culture assessments. While annual reviews maintain incremental relevance, major updates typically occur in 3-5 year



Ethics with a positive approach:

Significant organizational milestones, such as important anniversaries or the achievement of major strategic goals, provide natural platforms to reinforce and renew ethical commitments. These moments of celebration can be used to launch updated Codes with greater impact and organizational responsiveness.



Generational changes:

As new generations enter the workforce, their expectations and ways of communicating evolve. An effective Code should resonate with all employees, requiring periodic adjustments in tone, format, and delivery channels.

cycles, fundamentally re-examining the Code's structure, approach, and effectiveness.

Integration with the corporate governance calendar is essential. The Board of Directors should schedule a formal consideration of the Code at least annually, ideally in the first quarter of the fiscal year. The Audit Committee should include quarterly reviews of ethical reporting and semi-annual evaluation of program effectiveness. Code training should be systematically integrated, with **induction sessions for new employees** within their first 30 days, **annual refresher for all employees**, and **additional specific training for high ethical risk roles**.



Staying Relevant in Changing Contexts

The fundamental challenge is to keep the Code relevant without compromising its stability. This requires structured flexibility through stable fundamental principles that rarely change, specific policies that can be updated more frequently, and agile processes for minor updates. **Continuous monitoring of indicators** such as the use of ethical resources, types of queries received, and perceptions of ethical culture helps identify when the Code is losing relevance. The key is to allow for gradual evolution rather than revolutionary changes that can lead to organizational confusion and resistance.

Integration with Board Committees:

The Audit Committee typically assumes primary responsibility for oversight of the ethics program, including the Code. The Risk Committee, where it exists, should consider ethical risks as an integral part of its mandate, ensuring that the Code adequately addresses the risks identified. The Compensation Committee should ensure that incentive systems align with and reinforce the principles of the Code.

Synchronization with Other Processes

The effectiveness of the Code is maximized when synchronized with other key organizational processes:

Strategic Planning: The annual strategy review should explicitly consider ethical implications of new strategic directions. Significant strategic changes should trigger a review of the Code to ensure continuous alignment.

Internal Audits: The annual audit plan should include periodic reviews of aspects of the ethics program. These audits not only verify compliance but identify opportunities for improvement.

Performance Evaluations: Performance evaluation cycles must incorporate explicit consideration of ethical behavior and adherence to the Code. This integration reinforces that ethical behavior is a fundamental performance expectation, not an optional one.

Risk Management: Periodic updates of the risk matrix should consider emerging ethical risks that may require attention in the Code. This integration ensures that the Code evolves with the changing risk profile of the organization.

5. IMPLEMENTATION CHALLENGES AND CRITICAL SCENARIOS

Successful implementation of a Code of Ethics requires anticipating and preparing for the inevitable obstacles and challenging scenarios that will arise. This chapter consolidates the analysis of common problems, red flags, and response strategies for critical situations.



Recognizing Warning Signs

Organizations should be alert to early indicators of problems in implementation. The **silent release** of the Code, without active senior leadership involvement or meaningful communication events, **sends a clear message that it is not truly important**. The paradox of ethical silence occurs when reporting channels remain consistently unused, typically indicating fear or mistrust rather than absence of problems.

The **disconnect between proclaimed values and the daily actions of leadership** fatally erodes the credibility of the program. When training becomes a mechanical exercise with no real involvement, or when there are no clear metrics of effectiveness, the program is failing in its fundamental purpose.



Navigating Critical Scenarios

Resistance to Change Resistance can come from multiple organizational levels. In leadership, it arises when the Code is perceived as a limitation on their autonomy. In middle management, due to concerns about additional administrative burden. Among employees, for cynicism based on previous experiences or fear of retaliation. Addressing this resistance requires two-way communication that clearly articulates the “why” of the Code, early engagement of representatives at all levels, and phased implementation with pilot programs that demonstrate concrete benefits before overall expansion.

Limited Capacity. Many organizations face limitations in technical knowledge, time, or resources. Capacity building should be seen as a long-term investment through condensed executive training programs, individual *mentoring* for key leaders, and strategic incorporation of external *expertise*. For limited resources, sector collaboration sharing development costs, partnerships with local academic institutions, and effective use of technology can provide cost-effective solutions.



Having complaints is not always negative:

Healthy organizations typically experience an initial increase in reporting after the launch of a new Code or reporting channel, as employees test the system and gain confidence. Prolonged silence suggests that employees do not believe reporting is safe or helpful, preferring silence to risking retaliation or being ignored.

Cultural Divergences. The tension between global standards and local practices requires identifying truly universal ethical principles while allowing flexibility in practical implementation. For example, in societies with strong family ties, absolutely prohibiting family relationships in the company may be impractical. The solution requires policies that recognize these realities by establishing appropriate safeguards such as full transparency and restrictions on direct reporting lines. In markets with high economic informality, staggered due diligence processes and supplier development programs that facilitate gradual formalization are needed.



Prevention and Correction Strategies

Active monitoring through regular ethical climate surveys, analysis of patterns in reports, and cultural audits allows early identification of problems. Continuous improvement cycles should include post-incident reviews that generate concrete learnings, agile processes for updates when gaps emerge, and effective mechanisms for translating feedback into visible actions.

Visible and Consistent Leadership is Critical. Leaders should regularly discuss ethics, set an example of the behavior expected of them – particularly when making difficult decisions – and take responsibility when they fail to meet standards. Finally, organizations must cultivate a learning culture that sees minor ethical errors as opportunities for collective improvement, creating safe spaces to discuss dilemmas and share lessons learned.

Successful navigation of these challenges requires recognizing that the implementation of the Code is a **process of continuous cultural change**, not a project with an end date. Organizations that embrace this complexity with humility, creativity, and an unwavering commitment to integrity are the ones that manage to build truly sustainable ethical cultures. As **IDB Invest** states, a code of ethics is never a substitute for a poor business plan but recognizing warning signs early on and acting decisively can make the difference between a transformative code and one that is merely for show.



Building bridges between the global and the local:

Success in navigating divergences between global standards and local contexts requires a “*glocalization*” approach – thinking globally while acting locally. This involves upholding universal ethical principles while developing practical implementations that respect and adapt to legitimate local realities.

6. ANNEXES AND RESOURCES

Glossary of Terms

Below, we present a comprehensive glossary of the terms used in this document, including the terminological variations employed in the largest Latin American countries.

Term used	Meaning	Variations by country/region
Senior Management	A group of top-level executives who report directly to the General Manager/ CEO, including vice presidents and executives in key areas	Argentina: Gerencia Superior, Gerencia Chile: Plana Ejecutiva Brazil: Alta Administração, Diretoria Executiva Anglicism: Management.
AML/CFT	Acronym for Anti-Money Laundering and Combating the Financing of Terrorism (or AML/CFT).	This Anglicism is widely accepted.
CEO (Chief Executive Officer)	A company's highest executive authority, responsible for day-to-day management	This Anglicism is widely accepted. Mexico: Director General Argentina: Gerente General Colombia: Presidente Ejecutivo, Presidente (in large companies) Brazil: Diretor Geral, Diretor Presidente
Conflict of Interest	Situation in which personal interests may interfere with the interests of the company	Used consistently in all countries
Independent Director	Board member with no material relationship to the company, management, or controlling shareholders	Used generally throughout the region, except in Mexico: Director Independiente Chile: Director Externo Independiente
Board of Directors	Collegiate body chosen by the shareholders to oversee company management	Argentina, Chile: Directorio, Junta Directiva Colombia, Venezuela: Junta Directiva Peru: Directorio Brazil: Conselho de Administração
Due Diligence	Comprehensive investigation and audit process carried out by a company or investor before finalizing a major transaction	The Anglicism "Due Diligence" is widely accepted.
Ethical nudges	Social norms that seek to highlight prevalent ethical behavior to incentivize it.	
FCPA	Abbreviation for Foreign Corrupt Practices Act. It is a U.S. law enacted in 1977 that prohibits U.S. companies and individuals from bribing foreign officials to obtain or retain a business.	This Anglicism is widely accepted.
Investor	Person or entity that contributes capital to the company expecting a return	Southern Cone: Inversor Brazil: Investidor
KPI (Key Performance Indicators)	Critical performance metrics used to measure progress toward objectives	This Anglicism is widely accepted. Alternatives: Key performance indicators, Performance metrics
President of the Board of Directors	The person who presides over and leads Board meetings.	Argentina, Chile: Presidente del Directorio Colombia: Presidente de la Junta Brazil: Presidente do Conselho
Stakeholders	All parties affected by the company	This Anglicism is widely accepted. Alternatives: Groups of interest, Interested parties.
Tone from the Top	An ethical and accountable culture fostered by the behavior of leaders.	

Annex I: Ethics in Cybersecurity

Primary Focus:

It focuses on protecting systems, networks, and data from unauthorized access, damage, or misuse. Its principles revolve around confidentiality, integrity, availability of information, and responsibility in the protection of digital assets.

Scope:

It addresses technology infrastructure security, cyber-attack risk management, privacy protection through security measures, and ethical response to data breaches. It is a matter of defense and resilience of the digital infrastructure.

Examples of Dilemmas:

What to do if a critical vulnerability is discovered but its immediate disclosure could expose users to increased risk? How do you balance safety with ease of use for employees? What is a company's ethical responsibility in the face of a data breach, beyond the legal?

Key Principles of Ethics in Cybersecurity:

Ethical cybersecurity is based on the following principles:

- **Confidentiality:** Protect sensitive information from unauthorized access. This includes customer data, intellectual property, and financial records.
- **Integrity:** Ensure that the data is accurate, complete and has not been modified without authorization. Information integrity is vital for decision making and trust.
- **Availability:** Ensure systems and data are accessible to authorized users when necessary. Unplanned outages can have serious ethical and operational consequences.
- **Transparency:** Being open and honest about cybersecurity practices, data collection and use, and how security breaches are managed. Transparency fosters credibility and collaboration.
- **Responsibility and Accountability:** Organizations and individuals must be held accountable for their actions in cybersecurity. This involves establishing clear lines of accountability, oversight mechanisms, and consequences for ethical failures.
- **Fairness:** Ensure that security measures do not inadvertently discriminate against specific groups of users or populations.
- **Damage Limitation:** Act to mitigate the damage caused by cybersecurity incidents and avoid actions that may cause disruption or undue distress.
- **Compliance and Continuous Learning:** Adhering to applicable laws and regulations and staying up to date on the latest threats and best practices to continuously evolve the security program.

Ethical implications of data breaches:

Data breaches represent one of the biggest threats to corporate integrity and carry serious ethical implications:

Loss of Trust: Clients, investors, and the public lose confidence in the company's ability to protect their information, which can have lasting effects on reputation and brand value.

Impact on Individual Privacy: Exposure of personal data can lead to identity theft, financial fraud and other malicious activities that directly affect people's lives.

Fiduciary Responsibility: Boards and senior management have a fiduciary responsibility to protect the company's assets, including data. Gaps may indicate failures in the oversight of this responsibility.

Legal and Regulatory Consequences: Cybersecurity failures can lead to significant fines and legal penalties, especially in jurisdictions with strict data protection regulations.

Responsible Cybersecurity Practices for Businesses:

To integrate cybersecurity ethics, organizations must have:

- **Leadership from above:** The Board of Directors and Senior Management must perceive cybersecurity as a strategic and governance effort, not just a technical one. Assigning cybersecurity responsibilities at the management level is critical.
- **Risk assessment and management:** Integrate cyber risk into the overall corporate risk matrix, prioritizing the most relevant risks to the organization.
- **Clear policies and procedures:** Develop and implement policies on data protection, access controls, incident response, and acceptable use of technology resources.

- **Awareness and training:** The “human chain” is often the weakest link. Train all employees in basic security principles, threat recognition (e.g., *phishing*), and best practices for using passwords and multi-factor authentication. Training must be ongoing and tailored to specific roles.
- **Incident response:** Have a detailed and proven incident response plan, which allows rapid containment, transparent communication with those affected and compliance with reporting obligations.
- **Audits and continuous monitoring:** Conduct periodic security audits and continuously monitor the network to identify vulnerabilities and suspicious activities.
- **Third-party management:** Ensure that suppliers, partners and contractors handling company data comply with compliant cybersecurity standards.



**Difference between
“Cybersecurity Ethics” and
“Digital Ethics and
Responsible AI”:**

Although “Ethics in Cybersecurity” and “Digital Ethics and Responsible AI” are intrinsically related and part of a broader umbrella of technology ethics, they differ in their main focus and can benefit from being treated separately, albeit with cross-references.

Annex II: Digital Ethics and Responsible AI

Primary Focus:

It deals with the broader ethical implications of the use of digital technologies and, crucially, Artificial Intelligence. This includes how AI and algorithms impact individuals and society, paying attention to equity, algorithmic bias, transparency of automated decisions, and accountability for the impact of AI.

Scope:

It goes beyond security to consider how digital technologies transform human interactions, decision-making, employment, data privacy (beyond security, including consent and use), and the social impact of automated systems.

Examples of Dilemmas: Is it ethical to use an algorithm for hiring decisions if it may have a racial or gender bias, albeit unintentional? How is the interpretability of an AI system’s decisions ensured? Who is responsible if an AI makes a mistake with serious consequences?

Artificial Intelligence and Digital Ethics: Navigating the Frontier of Trust

In today’s era, AI and digital technologies are rapidly transforming the business landscape by offering increased productivity and new opportunities. However, their deployment carries profound ethical challenges that require proactive governance and clear principles to ensure a positive and sustainable impact. Digital ethics is not just a matter of compliance, but a fundamental pillar for the reputation, *stakeholder* trust and long-term resilience of the organization.

Key Principles of Digital Ethics and Responsible AI:

The implementation of AI should be guided by the following fundamental principles, which are in line with international best practices and the specific characteristics of the Latin American and Caribbean context:

- **Transparency and Interpretability:** Understanding how AI systems operate is crucial. How data is collected, used, and shared should be clearly communicated, and, where necessary, decisions made by algorithms should be explainable in terms understood by humans. This includes appropriate disclosure of the functionality, strengths, and limitations of AI systems.
- **Fairness and Non-Discrimination:** AI systems have the potential to perpetuate or amplify existing biases if trained with faulty or unrepresentative data. It is imperative to ensure that algorithms are fair and unbiased, promoting diversity in training datasets and continuously monitoring for any discrimination or bias, paying particular attention to vulnerable populations.
- **Privacy and Security:** The protection of personal information is paramount. Robust cybersecurity measures, such as data minimization and encryption, must be in place to protect data throughout its lifecycle and ensure that individuals have control over how their data is used ([see Annex I](#)).
- **Accountability and Human Oversight:** AI must not operate in a vacuum. There must be clear human responsibility for AI systems, with monitoring mechanisms that allow human intervention in critical decisions and the establishment of audits and traceability of algorithmic actions.
- **Sustainability and Inclusion:** AI should be designed to be usable by a wide range of people, including those with barriers to access, and its environmental impacts (e.g. energy consumption of computer centers) should be assessed and managed. In Latin America, it is critical that AI reflects local socioeconomic and cultural realities, avoiding the exclusion of those operating outside formal systems.

Challenges and opportunities in Latin America and the Caribbean:

The Latin America and Caribbean (LAC) region is at an early stage in AI regulation and its regulatory landscape is still in its infancy. This presents a unique opportunity to develop frameworks that balance rights protection with innovation, adapting to local realities such as high informality and linguistic and cultural diversity. Businesses in LAC should lead the adoption of a “human rights-based” approach in the development and use of AI, ensuring that this technology is a positive force for social welfare and inclusive development.

AI Governance Alerts:

- **Lack of Technical Expertise:** Many countries and companies in the region lack the technical expertise and operational resources to audit AI systems or assess algorithmic risks. This requires investment in internal capabilities and, if necessary, the support of external experts.
- **Regulatory Fragmentation:** A fragmented regulatory environment in LAC can lead to “jurisdictional arbitrage,” where companies seek the most permissive regulations. Regional cooperation and coordination of standards are crucial.
- **Local Reality Disconnect:** AI systems trained with predominantly “Global North” data may not reflect LAC realities, which can lead to biased or irrelevant outcomes.

Annex III: Behavioral ethics and the importance of “social norms”

People tend to follow what they perceive “most do” or what is “approved” by their reference group. Ethical “nudges”, which based on social norms, seek to highlight prevalent ethical behavior to incentivize it. Instead of just saying “Don’t steal,” you could say “95% of our employees have never taken office supplies for personal use.” In an integrity program, instead of just listing sanctions, you can highlight that “most teams proactively report their conflicts of interest.”

Understanding and Guiding Ethical Decisions

Traditional ethics often focus on how people *should* behave. However, “behavioral ethics” studies the systematic and predictable ways in which individuals, even well-meaning individuals, can deviate from ethical standards. Recognizing these psychological influences is crucial to designing a Code of Ethics that not only prescribes, but actually *guides* daily behavior.

Why do people deviate from their “moral compass”? Lessons from Social Psychology:

Several classic experiments in social psychology have demonstrated how situational factors and the influence of authority or group can lead individuals to act in ways inconsistent with their own values:



The Asch Conformity Experiment (Solomon Asch): This experiment showed how peer pressure from a group can lead an individual to settle for a clearly incorrect opinion. Participants, presented with questions designed for other “actor” participants to give an incorrect answer, often aligned themselves with the erroneous answers of the majority to avoid standing out or being ridiculed, despite knowing the correct answer.

Here, the loss of moral compass is due to social pressure and the desire for conformity. Although participants knew the correct answer, a significant portion of them **settled for the obviously incorrect answer from the majority of the group**. Their individual judgment and perception of reality were suppressed by the desire to fit in, avoid conflict, or not look different. The moral compass is not so much “lost” as “recalibrated” to align with the group, prioritizing social acceptance over objective truth or one’s own moral judgment.

Corporate Engagement: Illustrates the danger of “groupthink,” where the desire for consensus or peer pressure can stifle critical thinking and dissent, leading to ethically questionable decisions. Encourages the creation of a culture that values diverse perspectives and “*speak-up culture*.”



The Stanford Prison Experiment (Philip Zimbardo): This study simulated a prison environment, randomly assigning participants the roles of “guards” and “prisoners.” Within days, the “guards” engaged in abusive behavior and the “prisoners” showed signs of severe distress. It demonstrated how social roles and the power of the situation can lead “normal” people to commit harmful acts, even against their own moral convictions.

The “moral compass” deteriorates and is rapidly lost due to the **power of social roles, situational expectations, and dehumanization**. The “guards,” while not inherently sadistic, engaged in abusive and authoritarian behavior because the role empowered them, and the situation seemed to legitimize them. The dehumanization of the “prisoners” (who were stripped of their identity and humiliated) made it easier for the “guards” to stop seeing them as individuals worthy of respect, overriding their moral inhibitions. In this case, the situation and the imposed role were so powerful that they rewrote individual behavior norms, leading to actions that, in a normal context, would have been considered immoral.

Corporate Engagement: Highlights the risk that hierarchical roles or toxic organizational environments (where there are significant power imbalances) may influence behavior, leading to abuses of authority or the dehumanization of others. Stresses the need for robust oversight and safeguards against abuse of power.



The Milgram Obedience Experiment (Stanley Milgram): This study explored the willingness of individuals to obey orders from an authority figure, even when those orders conflicted with their personal conscience and involved inflicting harm on another person. A surprising percentage of participants administered electric shocks (simulated) to a “student” (an actor) to dangerous levels, simply because they were told to do so.

In this experiment, the “moral compass” is lost or ignored due to **perceived authority and dilution of personal responsibility**. The participants, despite showing signs of distress and concern for the “student” (who was an actor), continued to administer what they believed were painful and even deadly electric shocks. This happened because an authority figure (the experimenter) assured them that they were not responsible for the consequences, but the authority figure themselves. Obedience to external authority prevailed over the internal sense of right and wrong to inflict harm on another human being. Participants entered an “agentic state,” where they saw themselves as mere instruments for executing the will of another, exempting themselves from moral responsibility.

Corporate Involvement: Reveals how organizational hierarchies and perceived authority can influence employee behavior. It highlights the importance of autonomy, open communication, and the ability to question guidelines that contradict the personal moral compass.



Lindblom's Incrementalism Theory (Charles E. Lindblom): Originally developed as a theory for determining public policy and decision-making processes, this phenomenon describes how people can engage in unethical behaviors without realizing it, because transgressions occur in small steps, or “slips,” rather than an abrupt leap. A small act of dishonesty, if not corrected or challenged, can normalize and lead to progressively more serious acts. It is easier to justify a small deviation than a large violation.

Incrementalism dilutes the perception of the severity of the act. Each step is only “a little more” than the previous one, and the person gets used to the new normal, erasing the line that they previously considered unacceptable. Self-justification (“everyone does it” and “it’s no big deal”) gets easier with each step.

Example in a Company: An employee falsifies a lower figure in a report to meet a sales target. If there are no consequences and you “get away with it,” the next time the forgery could be a bit greater, and then involve others, until it becomes a systemic accounting fraud practice. In one project, a small time-saving safety shortcut could be accepted, then another, until the safety of the final product is severely compromised without anyone having made a “big” unethical decision in one fell swoop.



Moral Licensing Theory (various authors, including Daniel Effron): Occurs when a person, for having performed a good moral action (or simply for feeling like a “good person”), feels entitled or licensed to perform a less ethical action without feeling guilty or remorseful. The past good deed “buys” permission for a future bad deed.

It creates a moral imbalance: **“Since I've already done something good, I can afford to do this thing that's not so good.”** The moral compass is not lost, but “compensated for,” which can lead to inconsistent behaviors and the justification of questionable actions.

Example in a Company: A company invests a large sum in a highly visible corporate social responsibility initiative (e.g. reforestation). After receiving public praise for it, the same company might feel justified in exploiting a tax loophole or adopting less ethical practices in its supply chain, internally arguing that “we are already doing our part for society.” A further case would be that of an employee who donates to a charitable cause then feels justified in taking company office supplies for personal use, rationalizing the decision with “I’m already a good person.”



Bandura's Theory of Moral Disengagement (Albert Bandura): It is a psychological process by which individuals can disengage their internal moral standards to perform immoral actions without experiencing guilt or self-criticism. Albert Bandura identified several mechanisms, including:

- **Moral Justification:** Reinterpreting harmful behavior as morally acceptable (e.g., “I’m firing people to save the company, it’s for the greater good”).
- **Euphemistic language:** Using neutral or positive language to disguise harm (e.g., “downsizing” instead of mass layoffs; “process optimization” to hide safety cuts).
- **Advantageous comparison:** Comparing immoral actions to even worse actions to make one’s own seem acceptable (e.g., “stealing a little is not as bad as the multimillion-dollar fraud of the competition”).
- **Shifting responsibility:** Attributing responsibility to the authority or system (e.g., “just following orders”).
- **Diffusion of responsibility:** When there are many people involved, no one feels fully responsible (e.g., “the decision was made by the committee”).
- **Ignore or distort the consequences:** Minimize the harm caused (e.g. “no one was really harmed”).
- **Dehumanization:** Denying the humanity of victims (e.g. “it’s just numbers on a spreadsheet”).

It is an active mechanism of self-deception that allows the person to “deactivate” their empathy and ethical principles to carry out the action. It is not that the compass is lost, but that it is deliberately ignored or silenced through rationalizations.

Example in a Company: A company knows that its product has a minor defect but does not correct it because the costs would be very high. They use euphemistic language (“cosmetic defect”) and morally justify the decision (“if we don’t, we lose jobs”) while spreading accountability across various departments. Employees involved can disengage morally by minimizing potential harm to the customer.

Rather than just *saying* what is right or wrong, behavioral ethics seek to *design* the environment to facilitate the right decisions. Behavioral ethics teach us that, for a Code of Ethics to be truly effective, goodwill is not enough; a deep understanding of human psychology and an intelligent design of the organizational environment are needed.

Annex IV: Key performance indicators (KPIs) for Codes of Ethics and Integrity

Indicator Categories by Maturity Level

Indicator	Formula/Metric	Frequency	Complexity	Objective	
A. COVERAGE AND ADOPTION					
A1	Training Coverage by Tier	$(\text{Trained employees by tier} / \text{Total employees by tier}) \times 100$	Quarterly	Low	Ensure universal reach of the program
A2	Initial Certification Time	Average days from hire to full certification	Monthly	Low	Accelerate the ethical onboarding of new employees
A3	Annual Statement Completion Rate	$(\text{Completed statements} / \text{Total employees obligated}) \times 100$	Annual	Low	Measure formal commitment to the Code
A4	Critical Third-Party Coverage	$(\text{Third parties with ethical training} / \text{Total critical third parties}) \times 100$	Biannually	Average	Extend ethical culture to value chain
B. USE AND ENGAGEMENT					
B1	Ethical Enquiries by Employee	$(\text{Total enquiries} / \text{Total employees}) \times 100$	Monthly	Low	Measure proactive use of ethical resources
B2	Enquiry Response Time	Average hours between consultation and first response	Monthly	Low	Ensure timely support
B3	Consultation Ratio vs. Complaints	Preventive enquiries/Reactive reporting	Quarterly	Average	Evaluate preventive vs. reactive culture
B4	Access to Digital Resources	Unique visits to ethics portal/Total employees	Monthly	Average	Measure digital engagement
C. CASEMANAGEMENT					
C1	Resolution Time by Type	Average days from report to close by category	Quarterly	Average	Optimize procedural efficiency
C2	Schedule compliance	$(\text{Cases resolved in time} / \text{Total cases}) \times 100$	Monthly	Low	Ensure due process
C3	Research Trend	Annual % change in number of investigations	Annual	Low	Monitor trust in the system
C4	Founded Case Rate	$(\text{Founded cases} / \text{Total investigations}) \times 100$	Quarterly	Average	Evaluate the quality of the reporting system

Indicator	Formula/Metric	Frequency	Complexity	Objective
-----------	----------------	-----------	------------	-----------

D. CULTURAL IMPACT

D1	Ethical Environment Index	Weighted average of dimensions in annual survey (1-10)	Annual	High	Measure organizational ethical health
D2	Perception of safety	% of employees who feel confident reporting	Annual	High	Evaluate anti-retaliation effectiveness
D3	Knowledge of the Code	% of correct answers in post-training assessments	Quarterly	Average	Check for comprehension
D4	Trust in Ethical Leadership	% of employees who trust ethical behavior of leaders	Annual	High	Measure "tone from the top"

E. OPERATIONAL EFFICIENCY

E1	Cost per Investigation	Total investigation costs/ Number of investigations	Quarterly	High	Optimize resource allocation
E2	Prevention/Remediation Ratio	Prevention Budget/Remediation Budget	Annual	High	Prioritize preventive approach
E3	Updating Speed	Average days to update policies after regulatory changes	Annual	Average	Maintain regulatory relevance
E4	Program ROI	(Benefits Avoided + Value Generated) / Program Costs	Annual	High	Demonstrate business value

References

Levels of complexity

- Low: Easily available data, straightforward calculation.
- Medium: Requires specific tracking systems or additional analysis.
- High: Needs specialized surveys, valuation of intangibles or sophisticated analysis.

Recommended Frequencies

- Monthly: Critical operational indicators for daily management.
- Quarterly: Management indicators for course adjustments.
- Semiannual: Indicators of complex processes.
- Annual: Indicators of cultural and strategic impact.

Annex V: Example of ethical risk matrix

How to Use

This matrix makes it possible to identify, evaluate and prioritize specific ethical risks by functional area. Use a scale of 1-5 for probability (Prob.) and impact (Imp.), where 5 represents the highest risk, to determine the total Risk (Prob. x Imp.).

Identified Ethical Risk	Risk Description	Prob. (1-5)	Imp. (1-5)	Total Risk (P*I)	Existing Controls	Additional Controls Required	Respons.	Deadline
SALES AND BUSINESS								
Bribery of clients	Inappropriate payments or gifts to obtain contracts	3	5	15	Gift Policy, Monetary Limits	Specific training, client due diligence	Dir. Commercial	Q2 2025
Insider	Misuse of confidential client information	2	4	8	Confidentiality Agreements	Information Classification System	Dir. Commercial	Q1 2025
Unfair competition	Anti-competitive practices or defamation of competitors	2	4	8	Competency Code	Training in competition regulations	Dir. Commercial	Q2 2025
PURCHASING AND PROCUREMENT								
Supplier corruption	Receipt of undue benefits from suppliers	4	5	20	Selection committee, bidding process	Supplier evaluation system, staff turnover	Dir. Purchasing	Q1 2025
Conflicts of interest	Family/personal relationships with suppliers	3	3	9	Statement of conflicts	Relationship database, periodic review	Dir. Purchasing	Q1 2025
Favoritism	Non-objective selection of suppliers	3	3	9	Documented criteria	Process audit, transparent scoring	Dir. Purchasing	Q2 2025
HUMAN RESOURCES								
Discrimination	Biased hiring/promotion decisions	2	4	8	Diversity Policy	Training of unconscious bias, various panels	Dir. HR	Q1 2025
Workplace bullying	Hostile or intimidating work environment	2	5	10	Complaint Channel	Respect Program, Independent Investigations	Dir. HR	Q1 2025
Nepotism	Hiring based on personal relationships	2	3	6	Structured selection process	Selection committees with independent members	Dir. HR	Q2 2025

Identified Ethical Risk	Risk Description	Prob. (1-5)	Imp. (1-5)	Total Risk (P×I)	Existing Controls	Additional Controls Required	Respons.	Deadline
FINANCE AND ACCOUNTING								
Accounting fraud	Manipulation of financial records	2	5	10	Internal audit, segregation of duties	Automated controls, seat check	CFO	Q1 2025
Money laundering	Transactions of illicit origin	1	5	5	KYC, Transaction monitoring	Alert system, specialized training	CFO	Q2 2025
Tax evasion	Artificial structures to avoid taxes	2	4	8	External tax advice	Periodic review of structures, documentation	CFO	Q1 2025
OPERATIONS								
Environmental violations	Non-compliance with environmental regulations	3	4	12	Permits and licenses	Continuous monitoring, environmental audits	Dir. Operations	Q1 2025
Job security	Accidents caused by negligence in protocols	3	5	15	Security protocols	Regular inspections, near-miss reporting	Dir. Operations	Q1 2025
Product quality	Defective products that may cause damage	2	5	10	Quality control	Full traceability, independent testing	Dir. Operations	Q1 2025
TECHNOLOGY								
Cybersecurity	Personal or corporate data breach	4	5	20	Firewalls, antivirus, backup	Penetration testing, cybersecurity training	CTO	Q1 2025
Data privacy	Misuse of personal information	3	4	12	Privacy Policy	GDPR/LGPD compliance audit	CTO	Q1 2025
Misuse of systems	Unauthorized access to corporate systems	3	3	9	Set access controls	Multi-Factor Authentication, Audit Logs	CTO	Q2 2025

References

Critical Risks (15-25): IMMEDIATE ACTION

[Examples]

1. Supplier Corruption (20) - Procurement
2. Cybersecurity (20) - Technology

3. Customer Bribery (15) - Sales
4. Occupational Safety (15) - Operations

High Risks (10-14): PRIORITY ATTENTION

5. Accounting Fraud (10) - Finance
6. Workplace Harassment (10) - HR
7. Product Quality (10) - Operations
8. Environmental Violations (12) - Operations
9. Data Privacy (12) - Technology

Moderate Risks (5-9): CONTINUOUS MONITORING

10. Conflicts of Interest (9) - Procurement
11. Favoritism (9) - Procurement
12. System Misuse (9) - Technology
13. Discrimination (8) - HR
14. Insider Trading (8) - Sales
15. Unfair competition (8) - Sales
16. Tax evasion (8) - Finance

Quarterly Action Plan

Q1 2025 - Priority 1

- Implement enhanced due diligence of critical suppliers
- Perform comprehensive penetration testing
- Audit high-risk accounting processes
- Establish harassment investigation protocol

Q2 2025 - Priority 2

- Specific anti-corruption training for sales
- Comprehensive review of industrial safety protocols
- Implement independent product testing
- Privacy compliance audit

Review Frequency

- Full review: Annual
- Scoring Update: Semi-Annual
- Follow-up of action plans: Quarterly
- New risks identified: Immediate incorporation

Annex VI: Ethical Case Investigation Template

How to Use

This template provides a standardized format for documenting ethical research that ensures consistency, traceability, and organizational learning. It must be completed for each reported case, regardless of its complexity or final outcome.

CASE OVERVIEW

Field	Detail	Filling Notes
Case Number	[Auto-generated: Ethics-AAAA-###]	Format: Ethics-2025-001
Report Date:	[DD/MM/YYYY]	Date of complaint received
Opening Date	[DD/MM/YYYY]	When the investigation was formally initiated
Report Channel	Ethics <input type="checkbox"/> Line <input type="checkbox"/> Face-to-face <input type="checkbox"/> Email <input type="checkbox"/> Third Party <input type="checkbox"/> Website	Mark the channel used
Complainant	<input type="checkbox"/> Employee <input type="checkbox"/> Third Party <input type="checkbox"/> Anonymous <input type="checkbox"/> Customer <input type="checkbox"/> Other	Type of complainant type
Confidentiality	<input type="checkbox"/> Confidential <input type="checkbox"/> Anonymous <input type="checkbox"/> Identified	Required protection level

INITIAL CLASSIFICATION

Parent Category	Subcategory	Severity Level
<input type="checkbox"/> Conflict of interest	<input type="checkbox"/> Financial <input type="checkbox"/> Personal <input type="checkbox"/> Family <input type="checkbox"/> Commercial	<input type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High <input type="checkbox"/> Critical
<input type="checkbox"/> Discrimination/Harassment	<input type="checkbox"/> Sexual <input type="checkbox"/> Employment <input type="checkbox"/> Discrimination <input type="checkbox"/> Bullying	<input type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High <input type="checkbox"/> Critical
<input type="checkbox"/> Anti-corruption	<input type="checkbox"/> Bribery <input type="checkbox"/> Facilitation payment <input type="checkbox"/> Laundering <input type="checkbox"/> Fraud	<input type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High <input type="checkbox"/> Critical
<input type="checkbox"/> Use of resources	<input type="checkbox"/> Misuse of assets <input type="checkbox"/> Confidential information <input type="checkbox"/> Time	<input type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High <input type="checkbox"/> Critical
<input type="checkbox"/> Legal Compliance	<input type="checkbox"/> Contractual <input type="checkbox"/> Environmental <input type="checkbox"/> Labor <input type="checkbox"/> Regulatory	<input type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High <input type="checkbox"/> Critical
<input type="checkbox"/> Other	[Specify]	<input type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High <input type="checkbox"/> Critical

Severity Level Justification:

[Briefly explain why this level of severity was assigned, considering:

- Potential impact on the organization

Number of affected individuals

- Legal or regulatory exposure

Reputational risk]

CASE DESCRIPTION

Summary of Reported Facts:

[Objective description of the facts as reported, without initial interpretations. Include: what happened, when, where, who was involved]

Persons involved:

Name/Code	Position	Department	Role in the Case
[Identification]	[Position]	[Area]	<input type="checkbox"/> Reported <input type="checkbox"/> Witness <input type="checkbox"/> Victim
[Identification]	[Position]	[Area]	<input type="checkbox"/> Reported <input type="checkbox"/> Witness <input type="checkbox"/> Victim

Potentially Violated Policies: Code of Ethics and Integrity - Section: _____ Conflicts of Interest Policy Anti-Corruption Policy Diversity and Inclusion Policy Internal Work Regulations Other: [Specify]

INVESTIGATION PROCESS

Research team:

Name	Position	Role in the investigation	Date Assigned
[Name]	[Position]	<input type="checkbox"/> Principal Investigator <input type="checkbox"/> Specialist <input type="checkbox"/> Support	[DD/MM/YYYY]
[Name]	[Position]	<input type="checkbox"/> Principal Investigator <input type="checkbox"/> Specialist <input type="checkbox"/> Support	[DD/MM/YYYY]

Research Schedule:

Activity	Planned date	Actual Date	Person responsible	Status
Complainant Interview	[DD/MM/YYYY]	[DD/MM/YYYY]	[Name]	<input type="checkbox"/> Pending <input type="checkbox"/> Completed
Respondent Interview	[DD/MM/YYYY]	[DD/MM/YYYY]	[Name]	<input type="checkbox"/> Pending <input type="checkbox"/> Completed
Document review	[DD/MM/YYYY]	[DD/MM/YYYY]	[Name]	<input type="checkbox"/> Pending <input type="checkbox"/> Completed
Witness interviews	[DD/MM/YYYY]	[DD/MM/YYYY]	[Name]	<input type="checkbox"/> Pending <input type="checkbox"/> Completed
Evidence analysis	[DD/MM/YYYY]	[DD/MM/YYYY]	[Name]	<input type="checkbox"/> Pending <input type="checkbox"/> Completed

Evidence Collected:

Type of evidence	Description	Source	Date of issue	Relevance
<input type="checkbox"/> Documentary	[Specify]	[Origin]	[DD/MM/YYYY]	<input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low
<input type="checkbox"/> Testimonial	[Specify]	[Person]	[DD/MM/YYYY]	<input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low
<input type="checkbox"/> Digital	[Specify]	[System]	[DD/MM/YYYY]	<input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low
<input type="checkbox"/> Physics	[Specify]	[Location]	[DD/MM/YYYY]	<input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low

FINDINGS AND CONCLUSIONS

Factual findings

[List the facts that could be verified during the investigation, based only on verifiable evidence]

- 1.
- 2.
- 3.

Compliance Analysis:

Policy/Rule Evaluated	Complies	Does not Comply	Remarks
[Policy Name]	<input type="checkbox"/>	<input type="checkbox"/>	[Specific details]
[Policy name]	<input type="checkbox"/>	<input type="checkbox"/>	[Specific details]

Final Conclusion:

- FOUNDED CASE** - Policy/rules violation found
- UNFOUNDED CASE** - No violation found
- PARTIALLY FOUNDED CASE** - Some proven violations
- INSUFFICIENT EVIDENCE** - Could not be determined with certainty

Rationale for Conclusion:

[Detailed explanation supporting the conclusion, referencing specific evidence and applied reasoning]

CORRECTIVE AND DISCIPLINARY ACTION

Immediate Actions Taken:

[Measures implemented during the investigation to protect people or mitigate risks]

Disciplinary Measures (if applicable):

Person	Measure applied	Rationale	Date of Application
[Name/Code]	<input type="checkbox"/> Verbal <input type="checkbox"/> Written <input type="checkbox"/> Suspension <input type="checkbox"/> Termination <input type="checkbox"/> Other	[Reasons]	[DD/MM/YYYY]

Systemic Corrective Measures:

[Changes in processes, policies, training, controls, etc., to prevent recurrence]

1. Action: [Description]

Responsible party: [Name]

Deadline: [MM/DD/YYYY]

2. Action: [Description]

Responsible party: [Name]

Deadline: [MM/DD/YYYY]

FOLLOW-UP AND MONITORING

Plan for Follow-Up:

Monitoring	Method	Frequency	Person responsible	Next Revision
Compliance with disciplinary measures	[Method]	[Frequency]	[Name]	[DD/MM/YYYY]
Implementation of corrective actions	[Method]	[Frequency]	[Name]	[DD/MM/YYYY]
Non-retaliation against complainant	[Method]	[Frequency]	[Name]	[DD/MM/YYYY]

Case Reporting:

Audience	Message	Channel	Person responsible	Date
Complainant	Resolution and next steps	[Channel]	[Name]	[DD/MM/YYYY]
Management	Executive Summary	[Channel]	[Name]	[DD/MM/YYYY]
Ethics Committee	Full Report	[Channel]	[Name]	[DD/MM/YYYY]

LESSONS LEARNED AND IMPROVEMENTS

Lessons Learned:

1. [Specific lesson about the case or process]
2. [Opportunity for improvement identified]
3. [Risk pattern detected]

Recommendations for Prevention:

1. [Specific recommendation]
2. [Proposed control improvement]
3. [Suggested process change]

Impact on Policies/Procedures: No change required Minor policy update Major review of integrity framework Development of new specific policy

Details: _____

FORMAL CASE CLOSURE

Closing Date: [MM/DD/YYYY]

Total Investigation Time: ____ calendar days

Approvals:

Role	Name	Signature	Date
Principal Investigator	[Name]	[Signature]	[DD/MM/YYYY]
Compliance Officer	[Name]	[Signature]	[DD/MM/YYYY]
[Other, if necessary]	[Name]	[Signature]	[DD/MM/YYYY]

File retention: Physical file stored in: _____ Digital file stored in: _____

Retention period: ____ years (according to retention policy)

ADDITIONAL INFORMATION

[Space for additional observations, special circumstances, or information that may be relevant to future cases]

ATTACHMENTS TO THE FILE

Original complaint Interview transcripts Revised documents Digital evidence (logs, emails, etc.) Technical or legal opinions Official communications Other: _____

Sources

IDB Invest, "IDB Invest Corporate Governance Tool" (2024)

Corporate Governance Development Framework, "Corporate Governance Progression Matrix" (2024)

Corporate Governance Development Framework, "Corporate Governance Assessment Tool" (2017)

IBGC, "Corporate Risk Management" (2020)

IFC, "The Moral Compass of Companies: Business Ethics and Corporate Governance as Anti-Corruption Tools" (2009)

ISO, "ISO 37000:2021 Governance of organizations — Guidance" (2021)

ISO, "ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements" (2022)

OECD, "G20/OECD Principles of Corporate Governance" (2023)

OECD, "OECD Guidelines for Multinational Enterprises on Responsible Business Conduct" (2023)

OECD, "OECD Due Diligence Guidance for Responsible Business Conduct" (2018)

OECD, "Corporate Governance and Business Integrity: A Stocktaking of Corporate Practices" (2015)

Transparency International, "Business Principles for Countering Bribery" (2013)

AUTHORIZATION:

"Copyright © 2025 Inter-American Investment Corporation ("IDB Invest"). This work is licensed under a Creative Commons CC BY 3.0 IGO license. The terms and conditions indicated at the URL link must be respected, and proper attribution must be given to IDB Invest. In addition to Section 8 of the above license, any mediation related to disputes arising under this license will be carried out in accordance with the WIPO Mediation Rules in effect at the time of the dispute. Any dispute relating to the use of IDB Invest's works that cannot be resolved amicably will be submitted to arbitration in accordance with the rules of the United Nations Commission on Trade Law (UNCITRAL) in effect at the time of the dispute. The use of the IDB Invest name for any purpose other than attribution and the use of the IDB Invest logo shall be subject to a separate written license agreement between IDB Invest and the user and are not authorized as part of this license. Please note that the URL link includes terms and conditions that are an integral part of this license.

DISCLAIMER:

The opinions expressed in this work are those of the authors and do not necessarily reflect the views of the Inter-American Investment Corporation, its Board of Directors, or the countries they represent.