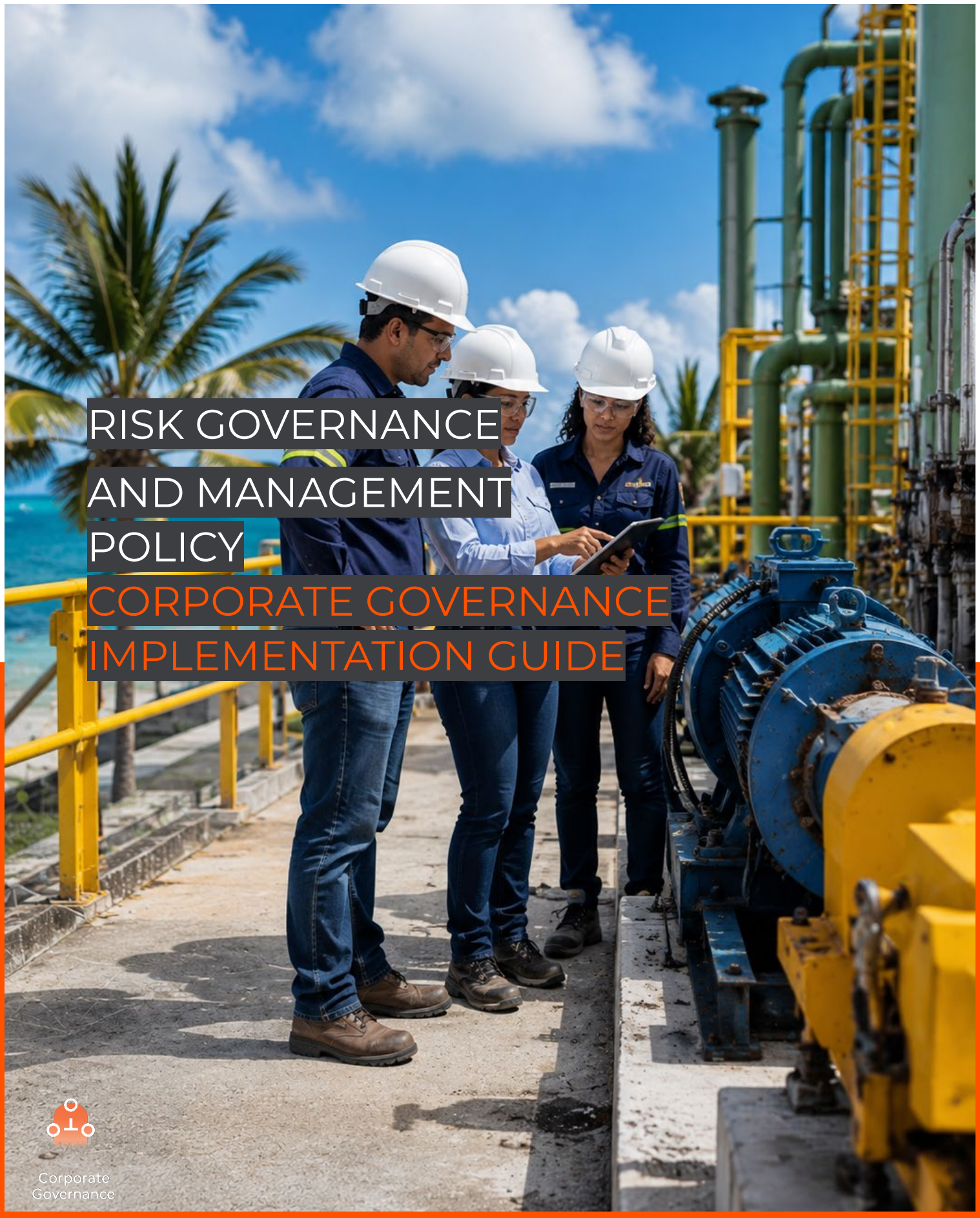
IDB | Invest



RISK GOVERNANCE AND MANAGEMENT POLICY

CORPORATE GOVERNANCE IMPLEMENTATION GUIDE

Corporate Governance

CONTENTS

About the Authors | Cefeidas Group

Cefeidas Group is an international advisory firm that helps its clients advance their objectives in Latin America. Cefeidas has worked with IDB Invest and the IDB for more than 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. FOUNDATIONS OF THE RISK GOVERNANCE AND MANAGEMENT POLICY

What is it and why is it indispensable?

The Risk Governance and Management Policy is the framework document that establishes how a company understands, organizes, and manages the risks it faces in pursuing its strategic objectives. It is not merely a technical manual for handling incidents; it is the Board of Directors' formal statement of how much risk the organization is willing to assume, who makes risk decisions, how risk is identified and measured, how the organization responds, and how risk is communicated throughout the organization.

Every company faces financial, operational, strategic, regulatory, reputational, technological, and sustainability risks, as well as—increasingly—risks arising from climate change and digital transformation. The difference between a company that thrives amid uncertainty and one that succumbs to it lies not in avoiding all risk, but in its ability to take risk consciously, on an informed basis, and within previously defined limits. This capability does not arise spontaneously; it requires a formal risk governance framework, and the Risk Governance and Management Policy provides that framework.

The policy answers three fundamental questions that every mature company should be able to answer clearly. First, which risks are relevant to our strategy? Second, how much of each risk are we willing to accept? Third, who is responsible for each aspect of risk management? Without formal, documented answers, business decisions rest on implicit assumptions, critical risks go unnoticed until they materialize, and disputes over who should have acted emerge too late and with damaging consequences.

Scope and application

The Risk Governance and Management Policy applies to the entire organization, without exception. This includes the Board of Directors and its committees, Senior Management, all business units and functional areas, subsidiaries and affiliates (with appropriate adaptations), and personnel at every level. Universal coverage is essential: risk cuts across the organization and does not respect hierarchies or organizational boundaries.

Key Concept: risk governance vs. risk management

Risk governance refers to the architecture for risk-related decision-making: who decides, based on what information, within which parameters, and subject to what oversight. Ultimate responsibility rests with the Board of Directors.

Risk management refers to the operational process of identifying, assessing, handling, monitoring, and reporting risks. It is an executive responsibility led by Senior Management and the Chief Risk Officer.

A sound policy integrates both dimensions: it defines governance (the structure) and guides management (the process).

The policy also applies, where relevant, to relationships with third parties: critical suppliers, strategic partners, contractors, and service providers whose conduct could create significant exposures for the company. In these cases, the policy guides the assessment of third-party risk and the incorporation of control requirements into the relevant contractual arrangements.

The roles described below are based on the Institute of Internal Auditors' Three Lines Model (see box), which allocates risk responsibilities across three complementary levels. The **first line** comprises business units and process owners, which generate and manage risk in their day-to-day operations and implement the corresponding controls. The **second line** comprises the Chief Risk Officer (CRO) and the Risk Department, together with other oversight and support functions such as Compliance, Information Security, and Business Continuity; its role is to provide methodology, aggregate monitoring, advice, and independent challenge to the first line without assuming its operational responsibilities. The **third line** is Internal Audit, which provides the Board with independent and objective assurance on the effectiveness of the overall framework.

Primary Roles Covered by the Policy

Board of Directors: approval of the policy and the Risk Appetite Statement, oversight of the framework, and ultimate accountability.

Risk Committee (or Audit and Risk Committee, depending on the structure): specialized oversight and in-depth consideration of risk matters on behalf of the Board.

CEO and Senior Management: operational implementation, resource allocation, and reporting to the Committee and the Board.

Chief Risk Officer (CRO) and Risk Department: second-line methodological leadership, aggregate monitoring, and reporting.

Process owners and business units: first-line operational responsibility for risk within their respective areas.

Internal Audit: third line, independent assurance on the effectiveness of the complete framework.

The Institute of Internal Auditors' Three Lines Model (IIA, 2020)

The Three Lines Model helps organizations identify the structures and processes that best facilitate the achievement of objectives and promote sound governance and risk management. See the model here.

One policy, multiple levels of sophistication

The existence of a policy does not mean that every company must have the same level of sophistication. A medium-sized family business undergoing professionalization may begin with a concise policy focused on the essentials: roles, a basic appetite statement, a taxonomy of principal risks, and a simplified process. What matters is that the Board formally approves the document and commits to its gradual evolution. The policy can become more sophisticated as the company matures.

Purpose of the Policy

The policy pursues interrelated objectives that together transform risk management from a reactive practice into a strategic capability of the company:

- **Establish a clear risk governance architecture**, defining roles, responsibilities and reporting lines that avoid gaps and duplication.
- **Articulate the company's risk appetite and tolerance** so that strategic and operational decisions are made within known and approved parameters.
- **Promote a consistent risk culture** in which identifying, escalating, and handling risks is a natural part of day-to-day work.
- **Ensure the integration of risk with the strategy and business plan**, preventing risk management from becoming an activity isolated from the decision-making process.
- **Ensure compliance with regulatory frameworks and best practices**, including COSO ERM, ISO 31000, and, where applicable, specific sector regulations.
- **Enable timely, useful reporting to the Committee and the Board**, with information that supports oversight and decision-making rather than merely informing.

Link to the pillars of good corporate governance

The Risk Governance and Management Policy directly puts the four fundamental pillars of corporate governance into practice, translating them from abstract principles into concrete, verifiable practices:

1. Transparency. The risk management policy strengthens transparency by defining what risk information must be reported, how often, and to whom. It also establishes formal communication channels among the first, second, and third lines and provides a basis for disclosing material risks in annual reports and investor communications.

2. Accountability. The policy promotes accountability by assigning specific responsibilities to every level of the organization, including the Board, its committees, the CEO, the CRO, and process owners. It also establishes the consequences of breaching risk limits and requires risk acceptance decisions to be documented, including identification of the person or body responsible for approval.

G20/OECD Principles of Corporate Governance (2023)

The 2023 revised G20/OECD Principles of Corporate Governance devote a specific section to **risk governance**. They establish that the Board is responsible for approving the risk management policy, defining risk appetite, overseeing the integrity of control systems, and ensuring that processes are in place to identify and promptly report material risks. The Principles emphasize the importance of the Board having the information, experience, and knowledge required to perform this function.

References to international standards

ISO 31000 — Risk Management. Defines the principles, framework, and risk management process applicable to any organization, sector, or type of risk. It emphasizes that risk management should be integrated (part of organizational activities), structured and comprehensive, tailored to context, inclusive (involving stakeholders), dynamic, based on the best available information, attentive to human and cultural factors, and continuously improved. Learn more here.

COSO Enterprise Risk Management (ERM). This framework provides a comprehensive perspective for integrating risk management with organizational strategy and performance. Learn more here.

3. Responsibility. The policy recognizes that risk management is a fiduciary duty of the Board of Directors and defines the duties of care and diligence that should guide risk-related decision-making. It also uses the Three Lines Model to allocate responsibilities clearly and consistently throughout the organization.

4. Fairness. The policy supports fairness by ensuring that risk-related decisions do not unduly favor one stakeholder group over another. It also protects minority shareholders by requiring formal approval of material exposures and ensures that conflicts of interest associated with risk decisions are properly identified, assessed, and managed.

Sectoral regulatory standards

Companies in regulated sectors (financial services, insurance, energy, pharmaceuticals, telecommunications, among others) must also observe the specific frameworks issued by their regulators. For example, in the financial sector, the Basel principles on risk management are mandatory. The company's policy must incorporate and harmonize these requirements, not contradict them.

Advantages by company type

Family Businesses	In family businesses, the policy plays a particularly valuable role in professionalization and institutionalization. Historically, these companies have managed the risk through the intuition of the founder or members of the family with executive roles. This approach, effective while the company is small and the risks are known, becomes unsustainable when the company grows, diversifies, incorporates non-family professional managers or attracts external investors. The policy allows the separation of risk decisions from family dynamics, establishes objective criteria for the escalation of significant exposures, and facilitates generational transition by documenting practices that would otherwise be tacit. In addition, the policy protects family assets by preventing individual decisions from exposing the company to risks that exceed the collective capacity to absorb them.
Unlisted non-family companies	For these companies, the policy typically facilitates the professionalization of the Board and accountability to investors or partners. A well-developed policy demonstrates to lenders, prospective investors, and strategic partners that the company has a mature decision-making framework, reducing risk premiums in the cost of capital, and facilitating future transactions such as funding rounds, acquisitions, or initial public offerings.
Publicly listed companies	For publicly traded companies, the policy is often an explicit or implicit regulatory requirement. Corporate governance rules issued by securities regulators in the region require, to varying degrees, a formal risk management framework, a Board-approved Risk Appetite Statement, and a Chief Risk Officer with direct access to the Board. Beyond compliance, the policy is essential to meeting the expectations of institutional investors, rating agencies, and analysts, all of whom require visibility into how the company's material risks are managed.
Listed family businesses	These companies combine the challenges of the two above categories. The policy plays a critical role in demonstrating that family dynamics do not compromise the independence and professionalism of risk management process, and that formal mechanisms exist to escalate to the Board any exposure that exceeds the approved limits, no matter who is responsible for the decision generated by the exposure.

Risk Culture

Risk culture is one of the most powerful determinants of the actual effectiveness of the risk management framework, and at the same time one of the most underestimated. Policies, processes, KRIs (Key Risk Indicators), and reports may be perfectly designed on paper, but if the organization does not share a coherent set of values, beliefs, and behaviors toward risk, the framework will fail precisely when it is needed most. In practice, major corporate crises are rarely explained by the absence of a formal framework; they are explained by a culture that tolerated ignoring what the framework revealed.

Responsibility for creating and maintaining a sound risk culture cannot be delegated by the Board of Directors. No Chief Risk Officer (CRO), however talented, and no Risk Department, however well resourced, can replace the effect that the behavior, decisions, and priorities of the Board and Senior Management have on how risk is understood and experienced throughout the organization. Culture is built from the top: the so-called "tone at the top" is the primary transmission mechanism and multiplier of the formal framework.

What it means, specifically, to generate risk culture from the Board

Beyond formal statements, generating risk culture is materialized in observable behaviors of the Board of Directors that the rest of the organization reads as signals about what is valued and what is tolerated. The Board directly assumes the following practices:

- **Model the expected behavior:** through its own decisions and conduct, the Board demonstrates what the organization should value. If the Board dismisses uncomfortable reports, the organization will learn to sugarcoat them; if it demands and discusses them seriously, the organization will learn to produce them rigorously.
- **Assign time and attention to risk:** the Board devotes significant space in its agendas to substantive risk discussion, not just formal document approval. An annual session is not enough; a recurring presence of the topic is required at regular meetings.
- **Ask difficult questions:** the Board actively questions the assumptions behind risk assessments, adverse scenarios, emerging risks and decisions that move away from approved appetite. The quality of questions shapes the quality of answers.

Culture Audit

Increasingly, Internal Audit is expected not only to assess processes and controls, but also to monitor organizational and risk culture. This "culture audit" provides the Board with independent evidence regarding the three dimensions discussed above, complementing the CRO's perspective. The scope, methodology, and reporting of Internal Audit are addressed in detail in the Corporate Governance Implementation Guide — Internal Audit Charter, which provides further guidance on this topic.

- **Support those who escalate risks:** the Board publicly supports the CRO and others who report uncomfortable exposures, even when their reports contradict Senior Management. Punishing the messenger is the fastest way to destroy a risk culture.
- **Align incentives:** the Board ensures that Senior Management's variable compensation arrangements incorporate risk considerations, not only performance. A system that rewards returns exclusively encourages excessive risk-taking, regardless of what the Policy says.
- **Allow constructive disagreement:** the Board creates space in which dissent on risk matters is legitimate and welcome. Cultures in which everyone agrees are the ones that produce the most spectacular failures.

The three observable axes of risk culture

To oversee risk culture systematically, the Board and the Risk Committee may assess it across three complementary dimensions—the same dimensions that Internal Audit typically analyzes when conducting a culture audit:

- **Tone at the top:** how the Board and Senior Management prioritize, communicate, and model risk management. What is the stated appetite, and how is it reflected in actual decisions? Are internal communications consistent with the approved Policy?
- **Day-to-day risk management:** what happens operationally within the organization. Are there regular meetings to discuss risks? Do managers escalate issues or conceal them? What is the quality of reports and the depth of discussion?
- **People management:** how talent processes reinforce or erode culture. Do incentive programs reward responsible risk behavior? Does performance assessment include risk management criteria? Is training systematic?

Signals of a weak risk culture

Some early signs of a weak risk culture that deserve attention from Board are:

- no substantive discussion on risk at the meetings of the Board and Committee;
- reports that only present good news;
- no reported events or "near misses" (suggesting underreporting, not their absence);
- frequent rotation or abrupt exit of the CRO or the Head of Internal Audit;
- resistance of management to the recommendations of the second and third line;
- variable compensation tied exclusively to financial results;
- silent tolerance of "minor" breaches.

When several of these signals coexist, the formal framework may be operating on a fragile cultural basis.

2. KEY COMPONENTS AND STRUCTURE

The following model presents a basic structure for the drafting of a Risk Governance and Management Policy. Companies are invited to adapt this model according to their specific context. Italics and gray background texts represent the suggested drafting model, while the annotations in the side or prominent boxes offer practical guidance to complete each section.

[Cover]

RISK GOVERNANCE AND MANAGEMENT POLICY

Contents:

CHAPTER I: GENERAL PROVISIONS

ARTICLE 1 — Subject

The purpose of this Policy is to establish the risk governance and management framework of [Company Name] by defining the principles, organizational structure, roles and responsibilities, risk appetite, and comprehensive process for identifying, assessing, handling, monitoring, and reporting the risks to which the Company is exposed in pursuing its strategic objectives.

ARTICLE 2 — Scope

This Policy applies to the Company and all its subsidiaries and affiliates (the "Companies"), its Board of Directors and committees, Senior Management, all employees, and, where relevant, contractors, critical suppliers, and third parties acting on behalf of the Companies.

Key Concept

If the company belongs to a group, define precisely which entities are covered by the policy. For subsidiaries in other countries, consider whether adaptations are required to reflect local regulation. Exclusions should be explicit and justified.

ARTICLE 3 — Definitions

For the purposes of this Policy, the following definitions apply:

a) Risk Appetite: the amount and type of risk the Company is willing to accept in pursuing its strategic objectives.

b) Risk Tolerance: the maximum level of risk the Company is willing to accept, including permissible variation from the Risk Appetite, before escalation or corrective action is required.

c) Risk Capacity: the maximum level of risk the Company can assume without compromising its solvency, operational continuity, or regulatory compliance.

d) Risk Culture: the set of risk-related values, beliefs, knowledge, attitudes, and behaviors shared by all employees.

e) Key Risk Indicator (KRI): a metric used to monitor exposure to a specific risk and flag deviations.

f) risk map: visual representation of identified risks, classified by their probability and impact.

g) Three Lines Model: an organizational framework that allocates risk responsibilities among operational functions (first line), oversight and support functions (second line), and Internal Audit (third line).

Key Concept

Definitions are critical to the interpretative consistency of the document. Avoid creating your own definitions for concepts that already have internationally recognized and justified standard definitions.

CHAPTER II: PRINCIPLES AND RISK CULTURE

ARTICLE 4 — Guiding Principles

Risk management in the Company is governed by the following principles:

a) Integration with strategy: risk management is an integral part of the strategic planning and decision-making process, not a separate activity.

b) Board leadership and commitment: the Board of Directors assumes ultimate responsibility for the risk management framework and demonstrates its commitment through its time, attention, and decisions.

c) Proportionality: the sophistication of risk management process is proportional to the complexity and materiality of the risks faced.

d) Timely, high-quality information: risk decisions are based on the best available information, communicated promptly to those who must act.

Key Concept

The principles articulate the company's philosophy of risk. They are useful in solving dilemmas not explicitly foreseen in the rest of the document. Adapt them to the words and priorities of your company.

e) *Open culture: early identification, transparent reporting, and constructive discussion of risks are encouraged without punishing the messenger.*

f) *Continuous improvement: the risk management framework evolves with experience, changes in the environment and maturity of the organization.*

ARTICLE 5 — Risk Culture

The Company actively promotes a risk culture characterized by:

a) *Proactive risk identification at all levels of the organization.*

b) *Timely escalation of exposures that exceed approved limits.*

c) *Clear accountability for risk management in every role.*

d) *Ongoing staff training in risk management.*

e) *Recognition and incorporation of lessons learned from incidents and near misses.*

f) *The integration of risk considerations into performance and compensation assessment processes.*

CHAPTER III: RISK GOVERNANCE STRUCTURE

ARTICLE 6 — Responsibilities of the Board of Directors

The Board of Directors is the Company's highest risk governance body and, in that capacity:

a) *Approves this Policy and its material updates.*

b) *Approves the Risk Appetite Statement and its associated categories, levels, and metrics at least annually.*

c) *Monitors the effective implementation of the risk management framework through the Risk Committee.*

d) *Ensures that the Company has the resources, systems, and qualified personnel required for risk management.*

e) *The CEO appoints the Chief Risk Officer (CRO), subject to prior approval or no objection from Board of Directors. The Board approves the CRO's mandate and responsibilities, periodically reviews its performance and must be consulted before any removal decision.*

f) *Receives and discusses periodic reports on the Company's risk profile, material exposures, breaches of risk appetite, and emerging risks.*

Fiduciary Responsibility

This is the Board's most important fiduciary responsibility in relation to risk. Ensure that the list reflects all decisions that only the Board may make and cannot delegate. If the company has a formal **Risk Committee**, specify which decisions may be delegated to the Committee and which remain with the full Board.

Note: Companies that, depending on the nature, scale and complexity of their operations and risks, determine that they have a complex risk profile, may adopt as an alternative that the Chief Risk Officer (CRO) is directly designated by the Board of Directors. In such case, sub-paragraph (e) should be amended to reflect that governance structure.

g) Approves any exposure that exceeds the approved risk appetite or directs that it be mitigated.

h) Actively promotes risk culture, demonstrating through its own behavior the expectations established in the Policy.

i) Assesses the effectiveness of the risk management framework annually, taking into account reports from Internal Audit and, where appropriate, external assessors.

ARTICLE 7 — Risk Committee

The Risk Committee [or Audit and Risk Committee, depending on the structure adopted] is a committee of the Board of Directors that supports the Board in carrying out its oversight responsibilities for the risk management framework. Its principal functions are the following:

a) Review this Policy and the Risk Appetite Statement and recommend their approval to the Board.

b) Monitor the implementation of the Policy and risk management framework.

c) Review the Company's risk profile and the Chief Risk Officer's periodic reports.

d) Conduct in-depth reviews of specific categories of material risk (financial, operational, cyber, climate, compliance, among others).

e) Assess the adequacy of the resources allocated to the function of risk management.

f) Review and validate key risk indicators (KRIs) and their limits.

g) Analyze breaches of risk appetite and recommend actions to the Board.

h) Coordinate with the Audit Committee (when different) on risk and control issues.

i) Report to the Board of Directors on its activities, findings, and recommendations.

ARTICLE 8 — CEO and Senior Management

The CEO is the chief officer responsible for the operational implementation of risk management framework and, in this capacity:

a) Ensures that this Policy is effectively implemented throughout the organization.

b) Allocates the human, financial, and technological resources required for risk management.

c) Designates the owners of each material risk category in coordination with the Committee and the Board.

Separate Risk Committee vs. Combined Audit and Risk Committee

Medium-sized companies often combine audit and risk functions in a single "Audit and Risk Committee" to make efficient use of Board members' time. The disadvantage is that the audit agenda tends to dominate. If this option is chosen, make the committee's name and the allocation of agenda time explicit.

Companies with complex risk profiles (financial services, energy, infrastructure, large listed companies) generally have separate committees. The main advantage is that each agenda can be addressed in greater depth.

d) Actively promotes risk culture from the top of the organization ("tone at the top").

e) Reports to the Committee and the Board on material risks and the status of Policy implementation.

f) Approves operational decisions within its delegated authority and within the approved Risk Appetite.

g) Promptly escalates to the Committee and the Board any exposure that exceeds approved limits or any material emerging risk.

Senior Management is collectively responsible for implementing the Policy in its respective areas and ensuring that the processes under its responsibility operate within the approved risk appetite.

ARTICLE 9 — Chief Risk Officer (CRO) and Risk Department

The Chief Risk Officer (CRO) leads the Risk Department and the second-line function. The CRO's principal responsibilities are to:

a) Design, maintain and update the methodological framework of risk management.

b) Coordinate the annual risk identification, assessment, and prioritization process throughout the Company.

c) Keep the corporate risk map and risk matrix consolidated.

d) Define Key Risk Indicators (KRIs) in coordination with process owners and monitor their development.

e) Support the Board and Committee in formulating the Risk Appetite Statement.

f) Report periodically to the Risk Committee and the Board on the risk profile, KRIs, breaches of risk appetite, and emerging risks.

g) Advise business units on integrating risk into their decisions.

h) Coordinate with Internal Audit, Compliance, and other control functions.

i) Promote risk management training throughout the organization.

j) Attend Risk Committee meetings as a nonvoting participant when requested.

Reporting line: the Chief Risk Officer reports functionally to the Risk Committee (and through it to the Board of Directors) and administratively to the CEO. This dual reporting line safeguards the CRO's independence to report any material matter promptly to the Board, even when it involves Senior Management.

Key Concept

Functional reporting to the Committee and administrative reporting to the CEO constitute international best practice. This structure ensures that Senior Management cannot silence the CRO when the CRO must report to the Board.

When is a dedicated CRO justified?

International practice recommends considering designating a dedicated CRO when:

- the company is publicly listed or plans to become listed;
- operates in a regulated sector with formal requirements (bank, insurance, energy, telecommunications);
- has operations in multiple countries or business lines;
- manages significant financial exposures;
- has experienced material adverse events in recent years; or
- financiers and investors explicitly demand it.

In medium-sized companies that do not yet have a formal CRO, the function may be assigned temporarily to the CFO or a part-time Risk Director until the maturity of the framework justifies a dedicated position.

ARTICLE 10 — Process Owners and Business Units (First Line)

Process owners and business-unit leaders constitute the first line of the Three Lines Model. They are operationally responsible for:

a) Identifying the risks inherent in their processes and operations.

b) Implementing the controls necessary to keep risks within the approved appetite.

c) Continuously monitoring the effectiveness of controls.

d) Promptly reporting any material event, incident, or near miss to the Risk Department.

e) Actively participating in annual risk identification and assessment exercises.

f) Collaborating with the Internal Audit in its revisions and implementing agreed remediation plans.

ARTICLE 11 — Internal Audit (Third Line)

Internal Audit is the third line of the risk governance model and provides independent and objective assurance on the effectiveness of governance, risk management, and internal control. [Its responsibilities in relation to this Policy are as follows:

a) Regularly assesses, through its risk-based work, the adequacy and effectiveness of Policy's implementation and the risk management framework.

b) Reports its findings, recommendations, and overall conclusion on the effectiveness of the framework to the Audit Committee.

c) Coordinate with second-line functions (Risk Department, Compliance, Information Security) without compromising its independence or assuming their operational responsibilities.

d) Report through the Audit Committee to the Board any risk accepted by Management that exceeds the approved risk appetite or tolerance.]

[Internal Audit's mandate, organizational independence, reporting lines, resources, scope of work, quality assurance, and other aspects are formalized in the Internal Audit Charter approved by the Board of Directors.]

CHAPTER IV: RISK APPETITE AND TOLERANCE

ARTICLE 12 — Risk Appetite, Tolerance, and Capacity

The Company adopts the following concepts to structure its approach to risk:

Internal Audit Charter

This Policy does not seek to duplicate the Internal Audit Charter. For details on purpose, organizational independence, functional and administrative reporting lines, the responsibilities of the Head of Internal Audit (HIA), the Annual Risk-Based Audit Plan, communication processes, quality assurance, and the function's operating model (in-house, co-sourced, or outsourced), see the Corporate Governance Implementation Guide — Internal Audit Charter.

Key Concept

The relationship between the Risk Committee and the Audit Committee (when separated) deserves special attention. Ideally, the chairs of both committees will coordinate their agendas and share information. In companies with a combined committee, this coordination is automatic.

- *Risk capacity represents the maximum risk the Company can assume without compromising its solvency, operational continuity, or regulatory compliance. It is determined according to the financial, human, operational, and reputational resources available.*
- *Risk Appetite is the amount and type of risk that the Company is willing to accept in pursuing its strategic objectives, within its risk capacity.*
- *Risk Tolerance establishes the acceptable level of variation from Risk Appetite before escalation or corrective action is required.*

The Company's Risk Appetite Statement is set out in Annex [X] to this Policy and is approved annually by the Board of Directors on the recommendation of the Risk Committee.

CHAPTER V: TAXONOMY AND RISK CATEGORIES

ARTICLE 13 — Risk categories

The Company adopts the following risk taxonomy, without prejudice to emerging risks that may be identified:

a) Strategic Risks: related to business model viability, investment decisions, mergers and acquisitions, and changes in the competitive environment.

b) Financial risks: including credit risk, liquidity, market, exchange rate, interest rate and counterparty.

c) Operational Risks: processes, people, systems, or external events. This includes Business Continuity Risk.

d) Compliance Risks: noncompliance with applicable laws, regulations, contracts, or standards.

e) Reporting Risks: errors or omissions in financial and nonfinancial information.

f) Technology and Cyber Risks: including Information Security, cyberattacks, use of artificial intelligence, technological dependence, and obsolescence.

g) Reputational Risks: loss of stakeholder trust.

h) Environmental, Social and Governance Risks (ASG/ESG): including physical and transitional climate risk, biodiversity, human rights and labor practices.

i) Fraud and Integrity Risks: including corruption, internal and external fraud, and money laundering.

j) Third-Party Risks: arising from critical suppliers, strategic partners, and service providers.

The taxonomy will be reviewed at least annually by the Risk Department and approved by the Risk Committee.

The **Risk Appetite Statement,** typically included as an annex to the Policy, is explained here. Annex I provides an RAS template.

Key Concept

The risk taxonomy is the common language that enables the entire organization to use the same concepts when discussing risk. It serves three functions: facilitating comprehensive risk identification, avoiding duplication (the same risk appearing in two categories), and enabling consistent aggregation of the risk profile at the corporate level.

The recommended structure is hierarchical. The first level contains the main categories (strategic, financial, operational, etc.). The second level breaks down each category into more specific subcategories. The third level, optional for more mature companies, identifies named individual risks.

Example hierarchy:

- Financial risk (Category)
  - Credit risk (Subcategory)
    - Portfolio concentration per customer (Named risk)

The taxonomy should reflect the business's material risks. Companies in specific sectors may require additional categories (for example, occupational health and safety risk in extractive industries).

CHAPTER VI: RISK MANAGEMENT PROCESS

ARTICLE 14 — Risk Management Process

The Company implements a continuous risk management process inspired by ISO 31000 and the COSO ERM frame, which includes the following steps:

a) Context setting: understanding the external and internal environment, strategic objectives and stakeholders.

b) Identification of risks: systematic detection of potential events that may affect the achievement of the objectives.

c) Risk analysis: understanding the causes, consequences and probabilities of each risk.

d) Risk assessment: comparison of the risk level with appetite and criteria established to prioritize risk handling.

e) Risk handling: selection and implementation of appropriate responses (avoid, transfer, mitigate, or accept).

f) Monitoring and review: ongoing monitoring of control effectiveness and changes in risks.

g) Communication and consultation: ongoing dialogue with relevant internal and external stakeholders.

h) Recordkeeping and reporting: documenting risks, decisions, and results and reporting them to the appropriate governing bodies.

Article 15 —Risk Handling

For each identified risk, the Company selects the most appropriate response, considering its cost, expected effectiveness, and the approved appetite. Handling options are:

a) Avoid: Discontinue the activity that generates the risk.

b) Transfer: transfer the risk to a third party (insurance, contracts, derivatives).

c) Mitigate: implement controls to reduce likelihood or impact.

d) Accept: consciously assume the risk, with the approval of the appropriate hierarchical level according to materiality.

Decisions to accept material risks (above the materiality threshold defined by the Board) are documented, justified, and reported to the Risk Committee.

CHAPTER VII: REPORTING AND ESCALATION

ARTICLE 16 — Periodic reports

The Risk Department prepares and presents the following periodic reports:

Key Concept

The process is cyclical and continuous, not linear. Its basic elements are:

Risk identification: the foundation of the process—an unidentified risk cannot be managed. Identification techniques include meetings with Senior Management and process owners; structured interviews; reviews of incidents and near misses; analysis of sector and peer literature; scenario analysis; reviews of external audits and assessments; and monitoring of the regulatory and competitive environment. Identification should be continuous and conducted at least annually.

Risk assessment: Analyzes the probability (that the risk materializes within a defined horizon) and impact (how severe the effect would be) to determine the risk level, represented in a heat map. It should distinguish between inherent risk (without considering controls) and residual risk (after applying existing controls), and some models incorporate the speed of materialization.

Risk handling: the response is defined according to cost, effectiveness, and risk appetite: avoid, transfer, mitigate, or accept the risk. Acceptance of material risks requires approval at the appropriate hierarchical level.

Continuous monitoring: performed through KRIs with thresholds and response plans, periodic reports to governing bodies, and independent audits and assessments (by the third line or external parties), providing information for effective oversight.

a) *Report [monthly or bimonthly] to the CEO: executive summary of KRIs, material events and breaches of risk appetite.*

b) *Report [quarterly] to the Risk Committee: material risk dashboard, KRIs evolution, emerging risks, mitigation plan status, and breaches of risk appetite.*

c) *Annual report to the Board of Directors: comprehensive review of the risk profile, results of the annual process of identification and evaluation, evaluation of the effectiveness of the framework, and recommendations for updating the Policy and the Risk Appetite Statement.*

d) *Ad-hoc reports: for material events, significant emerging risks or critical breaches of risk appetite that require immediate action.*

ARTICLE 17 — Escalation

Breaches of risk appetite are escalated under the following framework:

a) *Breaches within tolerance: managed by the first line, with notification to the Risk Department.*

b) *Breaches of tolerance that remain within capacity: notification to the CEO and the Risk Committee to define an action plan.*

c) *Material breaches that place solvency, continuity, or compliance at risk: immediate escalation to the Board of Directors.*

Escalation time frames are defined by the Risk Committee according to materiality and urgency and documented in the corresponding operating procedure.

Annex III helps to define responsibilities with a **RACI Matrix** of risk governance.

CHAPTER VIII: DOCUMENTATION AND SYSTEMS

ARTICLE 19 — Corporate Risk Matrix

The Company will maintain a Corporate Risk Matrix as the consolidated master record of identified and assessed risks. At a minimum, the Matrix will contain the following for each risk:

- *unique identifier;*
- *category according to approved taxonomy;*
- *name and description (cause, event and consequence);*
- *risk owner in the first line;*
- *assessment of inherent and residual probability and impact;*
- *existing controls;*
- *position against the approved Risk Appetite;*
- *associated key risk indicators;*
- *handling plan, including owners and deadlines; and*
- *last update date.*

Key Concept

The Corporate Matrix is the instrument that translates the Policy into day-to-day operations. Its quality determines the quality of the entire framework: if the Matrix is outdated or incomplete, reports to the Committee and the Board lose validity. A formal validation mechanism involving risk owners is recommended before each consolidation so that the Matrix does not reflect only the Risk Department's perspective. In medium-sized companies, the Matrix may be maintained in a structured spreadsheet; at higher levels of maturity, it may reside in a dedicated system.

The Risk Department is responsible for maintaining the Corporate Matrix, with documented input from risk owners. The Matrix will be updated at least quarterly and on an extraordinary basis in response to material events or significant changes in the external environment. The Matrix will be available at all times to the Risk Committee, the Board of Directors, and Internal Audit.

ARTICLE 20 — Key Risk Indicators (KRIs)

For each material risk identified in the Corporate Matrix, key risk indicators (KRIs) will be defined to allow monitoring of their development and timely warning of deviations from approved appetite. KRIs will meet the following criteria:

- *relevance to the risk they monitor;*
- *objective measurability with verifiable data sources;*
- *prospective (predictive) nature, when technically possible; and*
- *timeliness of production and reporting.*

Each KRI shall have:

- *a precise definition and calculation formula;*
- *a data source and person responsible for producing it;*
- *an established measurement and reporting frequency;*
- *tolerance thresholds differentiated in three levels (green: within appetite; amber: near limit; red: exceeds appetite); and*
- *a response plan for each alert level.*

KRIs will be proposed by the Risk Department in coordination with risk owners, validated by the Risk Committee, and reviewed at least annually. Aggregate KRI monitoring will be included in quarterly reports to the Committee and the annual report to the Board.

ARTICLE 21 — Systems, Tools, and Document Repository

The Company will have systems and tools proportionate to its size and complexity to support risk identification, assessment, handling, monitoring, and reporting. The systems will ensure information integrity, change traceability (audit trail), role-based access controls, and operational continuity through backups.

A centralized Document Repository for the risk management framework will be maintained, containing at least:

- *the current Policy and its previous versions;*
- *the current Risk Appetite Statement;*
- *the Corporate Risk Matrix;*

KRI vs. KPI

The distinction between a KRI (Key Risk Indicator) and a KPI (Key Performance Indicator) is important and frequently overlooked. KPIs measure past performance; KRIs anticipate future risk. A useful KRI detects pressure before a loss occurs. As a reference, a medium-sized company typically monitors between 20 and 40 enterprise-wide KRIs; a larger number tends to overwhelm the analytical capacity of the Committee and the Board. Thresholds should be recalibrated at least annually because outdated thresholds generate both false alarms and false negatives.

- *periodic reports to the Committee and the Board;*
- *the relevant minutes of the meetings of the Risk Committee;*
- *records of material events and lessons learned; and*
- *the Internal Audit framework reports.*

The Repository will be under the responsibility of the Risk Department. Document retention periods will comply with applicable legal and regulatory requirements, with a minimum of [X] years for documents supporting material decisions.

CHAPTER IX: REVIEW AND UPDATE

ARTICLE 22 — Annual and Event-Triggered Review

This Policy will be comprehensively reviewed at least annually by the Risk Department, with participation by the Risk Committee and final approval by the Board of Directors. The annual review will be aligned with the Company's strategic planning and budgeting cycle.

In addition to the annual review, extraordinary reviews will be conducted in response to the following triggers:

a) material changes in the business strategy or model;

b) significant corporate reorganizations, including mergers, acquisitions and divisions;

c) relevant regulatory changes affecting the risk management framework;

d) material adverse events showing weaknesses in the current framework;

e) critical recommendations from the Internal Audit or external evaluators; and

f) substantive changes to the international reference standards adopted by the Company.

The review will assess the validity and adequacy of the principles, the governance structure, the Risk Appetite Statement, taxonomy, KRIs, risk management process, and reporting flows.

ARTICLE 23 — Updating Process and Responsibilities

Modifications to this Policy shall be subject to the following process:

1) the Chief Risk Officer (CRO) prepares the proposed amendment, with the technical justification and corresponding impact analysis;

2) the proposal is submitted for prior consultation with the CEO, Senior Management, Internal Audit, Compliance, and Legal, and their comments are formally documented;

3) the Risk Committee reviews the proposal and comments received and issues a recommendation to the Board;

Key Concept

The annual review is a framework assurance exercise, not a rewrite. Under normal conditions, most elements remain unchanged, and only specific components are adjusted (threshold recalibration, incorporation of emerging risks, and adjustments to the RAS).

Frequent structural changes in the Policy are in themselves a warning signal, whether it is a poor original design or a lack of strategic stability.

Formally documenting that a review has concluded without material changes is as valuable as documenting changes: it demonstrates to external auditors, regulators, and funders that the review was actually performed.

4) *the Board of Directors approves the modification and instructs its communication and implementation.*

Material amendments to the Policy (those that alter the governance structure, Risk Appetite Statement, principal taxonomy, or critical escalation processes) always require approval by the full Board. Minor clarifying or formal amendments may be approved by the Risk Committee, with notice to the Board.

Any approved amendment will be formally communicated to Senior Management and the responsible parties no later than [30] business days after approval and incorporated into the Document Repository with an updated version-control record.

ARTICLE 24 — Continuous improvement

The Company adopts the principle of continuous improvement in its risk management framework. To this end, it will systematically incorporate the following sources of insight into the review process:

a) *lessons learned from adverse events, near misses, and breaches of risk appetite occurring during the period;*

b) *the findings and recommendations of the Internal Audit in its revisions of the framework;*

c) *the results of independent external evaluations when carried out;*

d) *emerging practices in comparable companies and in the development of international standards; and*

e) *contributions from relevant stakeholders, including investors, financiers, and regulators.*

The Risk Department will maintain a documented record of the continuous improvement process, including the sources considered, decisions to adopt or reject proposals, and actions implemented. This record will be reported annually to the Risk Committee.

CHAPTER X: FINAL PROVISIONS

ARTICLE 25 — Approval, validity and control of versions

This Policy enters into force upon approval by the Board of Directors, upon recommendation of the Risk Committee, and replaces any previous version or equivalent document. The Policy shall remain in effect indefinitely until modified or repealed by the Board.

A version-control record will be maintained for each approved version: version number, Board approval date, corresponding minutes reference number, summary of changes from the previous version, and document custodian.

ARTICLE 26 — Transitional provisions

[If, when this Policy is approved, the Company does not yet have all the structures and functions set out herein, the following transitional provisions will apply:

- *If the Risk Committee has not been formally established, its functions will be performed by the full Board of Directors or, if one exists, by the Audit Committee. The Company commits to formally establishing the Risk Committee, or formalizing a combined Audit and Risk Committee, within no more than [twelve (12)] months after approval of this Policy.*
- *If the Company does not have a dedicated Chief Risk Officer (CRO), the CRO's responsibilities will be assigned temporarily to [the Chief Financial Officer (CFO) / the Compliance Director / the CEO], preserving the functional reporting line to the appropriate Committee to the extent possible. A dedicated CRO will be appointed within no more than [eighteen (18)] months or when justified by changes in the risk profile.*
- *If the Risk Appetite Statement does not yet include quantitative metrics by category, an initial qualitative version will be approved and progressively enhanced over successive annual cycles.*
- *The operating procedures arising from this Policy will be developed and approved within no more than [six (6)] months after this document takes effect.]*

Key Concept

The transitional provisions are particularly relevant for medium-sized companies adopting their first Risk Governance and Management Policy before all ideal infrastructure is in place. Explicitly acknowledging these gaps and committing to specific deadlines for closing them is preferable to writing an aspirational Policy that does not reflect reality. The stated deadlines are illustrative; each company should align them with its actual capacity to execute. Without deadlines, transitional provisions tend to become permanent.

ARTICLE 27 — Custody, publication and communication

Formal custody of this Policy rests with [the Corporate Secretary / the Chief Risk Officer], who will ensure that the current version is available in the Document Repository and that historical versions are retained in accordance with the applicable retention requirements.

The Policy will be formally communicated to Senior Management, middle managers with risk management responsibilities, and all personnel whose roles are affected by its provisions. Communication will include an informative session tailored to the recipient's role.

The Policy will be incorporated into the induction program for new employees with relevant responsibilities. [For companies listed on the stock exchange, the Policy, or an executive summary, will be published on the corporate website and referenced in the annual corporate governance report.]

Key Concept

Communication is the activity that turns an approved document into a policy that is genuinely in force. Content and depth should be tailored to the audience: detailed sessions for Senior Management and those directly responsible; concise sessions for all personnel; and incorporation *into* new-hire onboarding. In listed companies, external publication strengthens accountability to investors and the market.

ARTICLE 28 — Annexes

The following documents form an integral part of this Policy and are considered to be in force along with it:

a) *[Annex I: Risk Appetite Statement approved by the Board of Directors.*

b) *Annex II: Corporate Taxonomy of Risks.*

c) *Annex III: RACI matrix of risk governance (assignment of responsibilities by activity).*

d) *Annex IV: Corporate Risk Matrix Template.*

e) *Annex V: Glossary of terms.]*

[Annexes I and II] may be updated by the Board of Directors on the recommendation of the Risk Committee without amending the main body of the Policy, given their dynamic nature. The other annexes may be updated by the Risk Committee with notice to the Board. Every Annex update will be communicated in accordance with Article 27.

Key Concept

Separating the more stable main body from the more dynamic annexes keeps the Policy current without requiring the Board to consider minor changes. This is useful in the calibration process for medium-sized companies that expect frequent adjustments during early cycles. It is critical, however, to establish clear rules on who may amend each component so that the separation does not allow unauthorized changes.

Key Concept: The Risk Appetite Statement (RAS)

The Risk Appetite Statement (RAS) is typically an annex to the Policy but warrants separate consideration because of its importance. The RAS translates the company's strategy and values into operational parameters that guide day-to-day decisions.

A well-designed RAS has three interrelated components: a **qualitative statement** articulating the company's overall risk philosophy; **statements by risk category** specifying the stance toward each type of risk (strategic, financial, operational, etc.); and **quantitative and qualitative metrics with corresponding limits** that allow adherence to the statement to be monitored.

Recommended appetite levels: An effective practice is to use a five-level scale of Risk Appetite by Risk Category:

- Risk Averse: Risks are not accepted in this category except in exceptional circumstances.
- Minimal: clear preference for low risk options, assuming only very low residual risks.
- Cautious: preference for safe options with low residual risk and limited opportunity for return.
- Open: willingness to consider all options and choose the one with the greatest likelihood of achieving the objective, taking risk into account.
- Hungry: willingness to consider innovative or more risky options that offer higher returns, consciously assuming the associated risk.

Rating source: HTM Orange Book (2023)

Key Concept: The Risk Appetite Statement (RAS) (continued)

Example Declaration by Category:

Reputational Risk: the Company adopts an averse stance toward reputational risk. Actions that could cause material reputational harm will not be accepted, even when they offer significant return opportunities. Decisions involving potential reputational impact must be escalated to the Risk Committee.

Financial Risk - Liquidity: the Company takes a cautious stance. It maintains a liquidity position that covers at least [X] months of operating needs in stress scenarios. Any material deviation requires the approval of the Risk Committee.

Innovation Risk: the Company adopts an open stance. It accepts innovation investments that may not generate positive short-term returns, within [X]% of the annual R&D budget, with quarterly monitoring by the Strategy Committee.

Frequent errors in drafting the RAS:

Three errors are common when writing the first Risk Appetite Statement:

i. generic declarations that apply equally to any company ("we seek to minimize risk by maintaining attractive returns"), which do not guide any real decision;

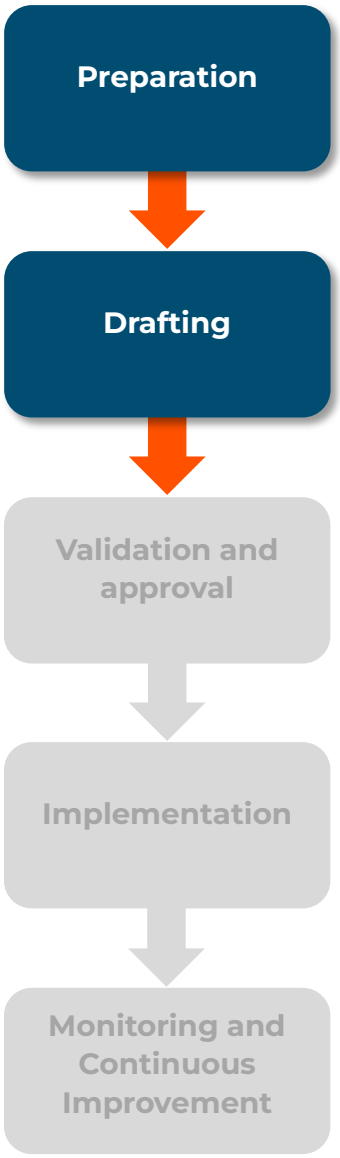
ii. statements without associated metrics, which prevent adherence from being monitored; and

iii. statements inconsistent with the approved strategy (declaring risk aversion when the strategy is aggressive growth).

A good RAS is specific, measurable and consistent with the strategy. See a model of the RAS in Annex I.

3. STEP-BY-STEP IMPLEMENTATION GUIDE

Developing and implementing the Risk Governance and Management Policy is a project that typically runs over a six- to twelve-month horizon, although companies with previous frameworks can do so in less time and start-ups working from scratch may require more time.



Preparation phase

1

Month 1

Action 1: Designate the project leader and obtain mandate from the Board

The first step is to appoint the project leader (ideally the CRO or, if no CRO exists, a member of Senior Management) and obtain a formal mandate from the Board of Directors. The mandate must define scope, timeline, resources, a Board member as focal point, and the expected deliverables: the risk management policy, Risk Appetite Statement, and implementation plan. Without this mandate, the project lacks the priority and authority needed to coordinate across different areas.

Action 2: Diagnosis of the current state of the risk framework

Before drafting the Policy, it is necessary to evaluate the current situation to identify existing practices, governance structures, related documents, and gaps in relation to best practices. The diagnosis is done through interviews, documentary review, benchmarking and, optionally, support from external consultants, culminating in a report that prioritizes the main areas of improvement.

Design phase

2

Months 2 to 4

Action 3: Define the structure of risk governance

Before drafting the Policy, key matters should be defined with the Board's participation, including the committee structure, appointment of the CRO, application of the Three Lines Model, and relationships with Compliance, Ethics, and Internal Audit.

"Quick wins"

Most companies already have risk management practices distributed in different documents. The aim is to consolidate and harmonize them in a coherent framework, taking advantage of existing ones to save time and reduce resistance to change.

Action 4: Draft Policy

With the governance defined, a clear, practical and company-friendly Policy is drafted. It is advisable to first prepare a complete draft and refine it in successive revisions to detect inconsistencies and gaps, especially when, in parallel, the Board defines the RAS (see action 5).

Action 5: Draft the Risk Appetite Statement

In parallel to action 4, the Board must define the level of acceptable risk by category and establish metrics and quantitative limits through workshops and historical and scenario analyses, then validate and formalize the Declaration.

Validation and approval phase

3

Months 5 to 6

Action 6: Consultation with key stakeholders

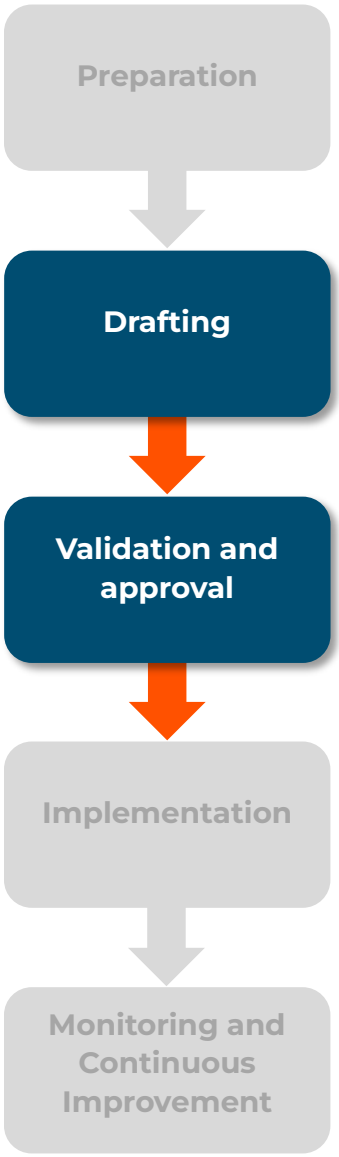
Before the draft is submitted to the Risk Committee for formal review, key stakeholders should be consulted to provide insights that strengthen the document: the CEO and members of Senior Management (operational feasibility); the Head of Internal Audit (alignment with the third line and audit plan); Legal (regulatory alignment); the Head of Compliance; and external auditors (for information).

Observations identify material problems before the document reaches the Board, which saves time and avoids the hassle of last-minute revisions. Each comment must be considered and, if not accepted, the reason must be documented.

Action 7: Review by Risk Committee and approval by the Board

Once validated by stakeholders, the draft is formally submitted to the Risk Committee (or the body performing that function) for review. The Committee typically requires one or two sessions to examine the most critical topics in depth: the Risk Appetite Statement, CRO responsibilities, and the escalation process. After the Committee's comments are incorporated, the Committee recommends that the Board approve the document.

The Board's approval is formally documented in the minutes. It is recommended that the session include an executive presentation of the document (not only its delivery), allowing the members to ask questions and fully understand the framework they are approving. Approval is the milestone that formally brings the Policy into effect.



Implementation Phase

4

Months 6 to 9

Action 8: Communication and training

A Policy that has been approved but is not understood will not bring about change. Communication must be systematic and multilayered: a formal announcement by the CEO or the Chair of the Board to the entire organization; differentiated training for different audiences (Senior Management, middle managers, process owners, and the Risk Department team); incorporation into new-employee induction programs; and permanent availability of the document in the company's repositories.

Action 9: Integration with existing policies and processes

The Policy does not operate in a vacuum. It must be integrated with the Risk Committee Charter (or Audit and Risk Committee Charter); the Chief Risk Officer's terms of reference; operating manuals and procedures for the various areas; strategic planning and budgeting processes; approval processes for investments, contracts, and commitments; variable compensation policies (incorporating risk considerations); and the annual Internal Audit plan.

Monitoring and continuous improvement phase

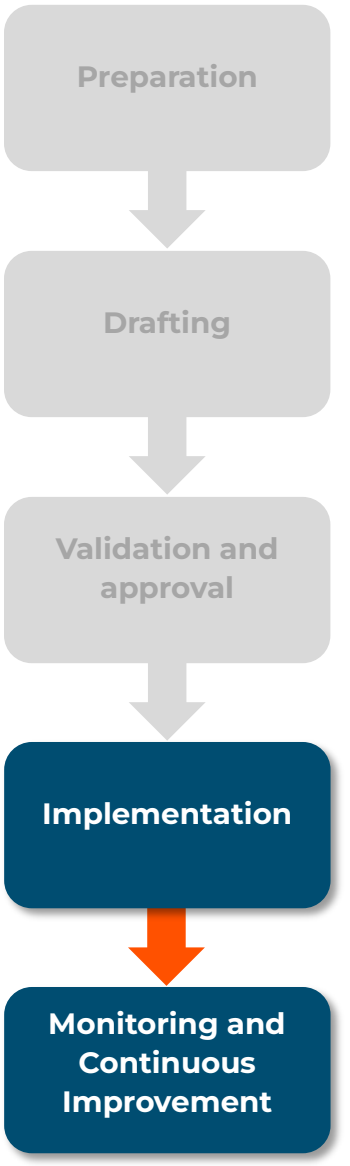
5

Continuous, from month 9

Action 10: Set the cycle for monitoring, reporting and continuous improvement

Implementation culminates in establishing a recurring operating cycle: the annual schedule for risk identification and assessment; the reporting frequency for the Committee and the Board (typically quarterly for the Committee and comprehensive annual reporting for the Board); the Policy review schedule (at least annually); and the process for reviewing and updating the Risk Appetite Statement (annually, aligned with the strategic planning cycle).

The first year of operation is the most important: it tests all the elements of the framework and reveals what works and what requires adjustments. It is recommended that the Risk Committee make a formal assessment of the implementation and propose the corresponding modifications to the Board.



Variable schedule

Companies that already have previous elements of risk management (a Committee that covers risk issues, a previous risk map, some scattered policy) can execute the project in four to six months. The difference is concentrated in phases 1 and 2.

4. TIME CONSIDERATIONS

Risk management is dynamic by nature, and the Policy must keep pace with that dynamism without losing stability.

Triggers for Developing or Revising the Policy

Beyond the general convenience of having a formal policy, there are specific triggers that increase the urgency of developing or reforming it. Recognizing these triggers in a timely manner allows you to anticipate the decision and avoid developing the policy under pressure conditions.

Strategic and business triggers

- **Corporate governance reform:** when a company decides to professionalize its governance (adding independent directors, forming committees, separating the founder's roles), it is a natural time to develop the policy.
- **Change in strategy:** a new strategy (entry into new markets, launch of business lines, digital transformation) generates new risk profiles that require formalization.
- **Corporate growth or transformation:** mergers, acquisitions, divisions, or reorganizations require updating of risk management framework.
- **Preparing for an initial public offering (IPO):** securities regulators and institutional investors require a formal framework before listing. Developing it in advance reduces costs and avoids delays.
- **Arrival of an external institutional or financial investor:** investment funds, development banks such as IDB Invest, and other institutional investors typically require the framework as a condition of their investment.
- **Generational transition in family enterprises:** the transition from one generation to another is the right time to institutionalize practices that depended on people.

Regulatory and external triggers

- **Regulatory change:** new requirements of corporate governance or risk management issued by sectoral regulators (values, banking, insurance, energy, telecommunications, health) that apply to the company.
- **Material adverse events:** significant frauds, serious operational failures, regulatory sanctions, reputational damage, or financial crises reveal weaknesses of the previous framework and require its revision.

Better to anticipate than to react

The worst time to develop a policy is under external pressure: a regulator demanding the document within thirty days, an investor whose transaction closing depends on its existence, or a crisis that exposed its absence. In these circumstances, the document is developed hastily, fails to capture the company's specific circumstances, and becomes a dead letter. Anticipating the triggers allows for methodical development of a useful, durable document.

- **Recommendations from external or internal auditors:** material findings on deficiencies in the risk management framework.
- **Material changes in the environment:** macroeconomic crises, pandemics, significant geopolitical changes, disruptive technological transformations, or intensification of climate risks.

Frequency of revision and update

The Policy should be periodically reviewed to maintain its validity without affecting the stability required for its implementation.

The recommended practice is to conduct an **annual comprehensive review**, aligned with the strategic planning cycle, to verify that the Policy, Risk Appetite, risk taxonomy, KRIs, processes, and reports remain adequate. The review is usually led by the CRO, validated by the Risk Committee and, where appropriate, approved by the Board.

In addition, **extraordinary reviews** should be made when relevant events occur, such as strategic changes, reorganizations, crises, regulatory changes, or entry into new markets, updating only the components affected.

In organizations with more mature risk management, some **risk categories** may be reviewed at different frequencies according to their level of dynamism—for example, quarterly, semi-annually, annually, or biennially.

Integration with the annual calendar of corporate governance

The Policy and its associated components should be coordinated with the rest of the annual governance calendar to avoid duplication, generate synergies and ensure that decisions are made on up-to-date and consistent information:

- **Q1:** Prior-year close. Review the year's risk profile, assess KRIs, and identify lessons learned. Begin the annual risk identification and assessment process.
- **Q2:** Consolidation of the annual risk map. RAS update proposal. Review by Risk Committee. Coordination with the annual Internal Audit plan.
- **Q3:** Board approval of the updated Risk Appetite Statement. Definition of KRIs and thresholds for the following year. Comprehensive review of the Policy and proposal of material updates.
- **Q4:** Board approves updates to the Policy. Integration with the budget and strategic planning cycle. Training to the Board and Committee on material changes. Preparation for year end.

5. IMPLEMENTATION CHALLENGES AND CRITICAL SCENARIOS

Warning Signs of Poor Implementation

Problems during the development phase.

The first warning sign appears when development of the document is **delegated entirely to an external consultant or the control team without the active involvement of the Board and Senior Management**. The result is a document that is technically correct but disconnected from the company's strategic reality—one that executive leadership does not view as its own and therefore does not champion or implement with conviction.

How to address this: Redesign the project as a co-creation exercise, not an outsourced assignment. Even when a specialized external consultant is hired, project leadership should rest with a senior internal figure backed by an explicit Board mandate. The consultant provides methodology and benchmarking; the company provides strategic context and makes the decisions. When Senior Management feels like it built the document, it champions it; when it feels like the document was simply handed over, it merely tolerates it.

Another warning sign is **regulatory copy-and-paste,** particularly common among companies under regulatory pressure. The policy is assembled by copying the model used by comparable companies—often in the financial sector—without adapting it to context. A framework designed for a bank with thousands of employees will be wholly unsuitable for a medium-sized family-owned industrial company, and vice versa.

How to address this: The initial diagnosis of the current state is the natural barrier to this problem, and it must be done before looking at any external model. The diagnosis answers three questions: what risks are truly material to our business; what practices of risk management already exist in the company, even

Multidisciplinary teams and invited auditors

Given the pace of change in the external environment, Internal Audit teams should combine different backgrounds (accounting, IT, engineering, ESG, and law). When a specific audit requires expertise the team does not possess, one useful practice is to engage a "guest auditor": a specialized professional hired temporarily or seconded from another area who joins the team under the direction of the Head of Internal Audit solely for that engagement. This is particularly useful for medium-sized companies with limited budgets.

if they are not formalized; and what effective capacity we have to operate the framework we approve.

Another **critical warning sign is the absence of a Risk Appetite Statement** or the use of generic drafting. If the policy discusses the risk management process extensively but does not include specific, measurable statements about how much risk the company is willing to assume by category, the document contains a structural gap that makes it operationally ineffective.

How to address this: When the Board resists committing to quantitative metrics, the answer is not to abandon the RAS but to break it down into two phases. The first RAS may be qualitative, classifying stance by risk category using the five-level scale (averse, minimal, cautious, open, hungry) without requiring numerical thresholds. This version is less intimidating and helps the Board build the habit of discussing appetite. Quantitative metrics are introduced at the next annual review, beginning with the most measurable categories (financial) and progressing to those that are less quantifiable (strategic and reputational). In addition, each qualitative statement must document its rationale: the internal or market evidence supporting it and the concrete decisions that would change if the stance were different. This exercise converts empty statements into operational commitments.

Problems during the implementation phase.

The most common sign of poor implementation is the **persistence of practices that predate the Policy**. Several months after approval, decisions are still made as before, reports to the Committee do not include risk information, KRIs are not monitored, and the Risk Appetite Statement is not used as a decision criterion. When this happens, the document exists in the repository but not in day-to-day operations.

How to address this: The policy displaces previous practices only when it is actively integrated into the decision-making processes in which those practices arise. Specifically, existing approval processes must change: investment memoranda, credit proposals, material contracts, and strategic decisions should include a risk section, the Risk Department's opinion, and verification of consistency with approved appetite. In parallel, reports to the Committee and the Board should be redesigned to include risk information systematically, including a KRI dashboard, trends relative to appetite, and emerging risks. One effective technique is to establish a cut-off date after which no relevant file may advance

without the formal risk section. In addition, during the first six to twelve months, the CEO should make implementation status a recurring item in regular meetings with Senior Management. Without this sustained push from executive leadership, organizational inertia will restore previous practices.

Another critical signal is the **isolation of the risk management function**. If the Risk Department operates in isolation, without interaction with business units, without participating in strategic decisions, and without presence in key management forums, its ability to influence is null and void and the implementation of the policy is limited to the preparation of formal reports that no one uses.

How to address this: The structural response is to integrate the Risk Department into decision-making forums, not only risk-oversight forums. This means formal participation by the CRO (or a delegate) in the Executive Committee or equivalent body, the investment or credit committee, quarterly strategy reviews, and development of the business plan and budget. The CRO should have an advisory voice and provide a written opinion when appropriate, not merely attend as an observer. In addition, the Department's operating model should combine two elements: a central core that maintains the methodology, corporate matrix, and aggregate reporting; and a network of "risk champions" distributed across business units who link to the first line and ensure that risk is discussed where exposures actually arise. Without this distributed network, even a technically strong central department will remain isolated.

The **lack of timely escalation** is a particularly dangerous warning sign. If breaches of risk appetite are not reported to the Committee and the Board within the established time frames, or are diluted among less relevant information, oversight is compromised and material risk grows silently until it materializes.

How to address this: Effective escalation requires explicit rules, protected channels, and clearly assigned individual responsibility. First, the policy must define precisely the thresholds that trigger automatic escalation, the maximum time between detection and communication (typically 24 to 72 hours, depending on severity), and the mandatory recipients at each level. Second, channels must exist that do not depend on Senior Management to operate: the CRO's functional reporting line to the Risk Committee; private executive sessions between the Committee and the CRO, without Senior Management present, at least annually; and the CRO's documented right to access the Committee Chair or the Board when necessary. Third, responsibility for escalation must be assigned personally: the CRO is responsible for escalating material exposures identified, and failure to fulfill this duty has explicit consequences in the CRO's performance assessment. Finally, the Committee must reinforce the correct behavior by publicly supporting the CRO when uncomfortable information is escalated. The moment the organization learns that escalation is safe is also the moment its escalation culture takes hold.

"What-If" Scenarios

"What if the Board does not approve the Risk Appetite Statement?"

Some Boards, particularly in family businesses or companies with still-developing governance practices, may be reluctant to define an explicit risk appetite. In these cases, a gradual approach is recommended: begin with a qualitative Risk Appetite Statement establishing the overall stance toward each risk category, then progressively incorporate quantitative metrics in subsequent reviews as the organization's risk management maturity increases.

"What if CRO reports a material risk that Senior Management minimizes?"

This scenario, unfortunately common, tests the integrity of the risk governance framework. The functional reporting line from the CRO to the Risk Committee (not only to the CEO) is the structural response: the CRO has the duty and the power to report directly to the Committee and, if necessary, to the Board, without Senior Management mediation. The policy must be explicit about this right and duty.

In addition, recommended practice includes private executive sessions *between* the Risk Committee and the CRO, without Senior Management present, at least annually. These sessions enable candid discussion of tensions that might otherwise remain unspoken.

Common Pitfalls

- **Confusing policy with procedures:** the policy should define principles, responsibilities, and general guidelines, while procedures describe how activities are performed. Keeping the two documents separate facilitates understanding and updating.
- **Underestimating the RAS:** a generic statement does not guide decision-making. It should clearly define the acceptable level of risk by category and evolve toward concrete metrics aligned with strategy.
- **Appointing a CRO without resources or support:** the risk management function requires adequate resources, access to the Committee or the Board, and an organizational structure that enables the CRO to perform the role effectively.
- **Producing overly long reports:** reports to the Committee and the Board should be concise, clear, and focused on critical information, with annexes where necessary.
- **Assigning second-line responsibilities to Internal** Audit: Internal Audit must preserve its independence as the third line. The Policy must clearly separate the responsibilities of Risk Management and Internal Audit.

“What if a material event occurs that exceeds the approved appetite?”

The response protocol should be provided for in the Policy. At a minimum, it should include immediate notice to the CEO and CRO; an extraordinary Risk Committee meeting within a short time frame (24 to 72 hours, depending on severity); an assessment of materiality and whether the Board must be notified; definition of a corrective action plan; communication with external stakeholders (regulators, investors, auditors) where appropriate; and a formal record of the event for ex post analysis and lessons learned.

The policy should also provide that decisions to accept exposures exceeding approved appetite may be made only by the body appropriate to their materiality: Senior Management may accept minor breaches within tolerance; the Committee approves material breaches within capacity; and the Board approves critical breaches.

“What if the Risk Committee identifies a structural weakness in the framework?”

In its oversight role, the Committee may occasionally determine that the current framework has structural weaknesses that operational implementation cannot resolve: insufficient resources, a CRO who is not suited to the role, deficiencies in the risk identification process, or gaps in the taxonomy. The response is to submit to the Board a recommendation to amend the Policy or related components, together with a clear diagnosis and remediation plan. As final approver, the Board decides and allocates the corresponding resources.

“What if a new emerging risk requires immediate attention?”

Emerging risks (cyber, climate, artificial intelligence, geopolitical) often arise between annual review cycles. The Policy should allow the Risk Committee to add new categories or KRIs without waiting for the annual review, subject to notice to the Board. This flexibility is essential: a rigid framework updated only once a year may fail to detect material changes in the environment in time.

Warning: the risk of a false sense of control

One of the most dangerous consequences of a poorly implemented framework is a false sense of control: the Board assumes that risks are being managed because a policy exists, but implementation is deficient and material risks are not detected or reported promptly. The consequences become apparent when a material event occurs and the defenses prove illusory. Active oversight by the Committee, independent assessments by Internal Audit, and, where appropriate, periodic external assessments are the tools that prevent this scenario.

6. ANNEXES AND RESOURCES

Glossary of Terms

Below is a comprehensive glossary of terms used in this document, including the terminological variations across major Latin American and Caribbean countries.

Term used	Definition
Risk Appetite	The amount and type of risk the organization is willing to accept in pursuing its objectives. Variant: "Apetito al Riesgo" (used interchangeably).
Risk Capacity	The maximum level of risk the organization can assume without compromising its solvency, continuity, or compliance.
Risk Committee	A Board committee specializing in oversight of the risk management framework. In medium-sized companies, it is frequently combined as an "Audit and Risk Committee."
Board of Directors	A decision-making body elected by shareholders to oversee management of the company. Also known as Junta Directiva (Colombia, Venezuela), Directorio (Chile, Peru, Argentina, Uruguay), or Consejo (Mexico, Spain).
Risk Culture	Shared values, beliefs, knowledge, attitudes, and behaviors concerning risk.
Risk Appetite Statement (RAS)	A Board-approved document defining the qualitative and quantitative stance toward risk.
Risk Department	Organizational unit under the CRO. Variants: Departamento de Riesgos, Dirección de Riesgos, Gerencia de Riesgos, Área de Riesgos, Función de Riesgos.
Escalation	The formal process through which an exposure or event is elevated to the appropriate hierarchical level for attention. Variant: Reporte ascendente (upward reporting).
Chief Risk Officer (CRO)	The senior executive responsible for the risk management function. Variants: Director de Riesgos, Gerente de Riesgos, Oficial Principal de Riesgo, Jefe de Riesgos.
KRI (Key Risk Indicator)	A metric used to monitor exposure to a risk and flag deviations. Distinct from a KPI (Key Performance Indicator).
Risk Map	Visual representation of the risks identified according to probability and impact. Variants: Mapa de Riesgos, Matriz de Riesgos, Mapa de Calor
Three Lines Model	The IIA's organizational framework (2020), which allocates risk responsibilities among the first line (operations), second line (oversight and support), and third line (Internal Audit). It replaces the former "Three Lines of Defense Model."
First Line	Functions that generate and manage risk in their day-to-day operations: business units, operating processes, and process owners.
Emerging Risk	A new or evolving risk whose profile is not yet fully understood. Examples include advanced cybersecurity, climate transition risks, generative AI, and geopolitical risks.
Inherent Risk	The level of risk in the absence of controls.
Residual Risk	The level of risk after applying existing controls.
Second Line	Functions that oversee and support the first line: Risk Management, Compliance, Information Security, among others.
Risk Taxonomy	Structured classification of the organization's risk categories.
Third Line	Internal Audit, which provides independent assurance on the effectiveness of the overall framework.
Risk Tolerance	Acceptable variation from risk appetite before escalation is required.
Tone at the Top	Behavior and communications by the Board and Senior Management that shape organizational culture.

Annex I: RAS Template

The following template may be adapted by each company to prepare its Risk Appetite Statement. It should be reviewed with local legal counsel before use.

RISK APPETITE STATEMENT — [Company Name]

Approved by the Board of Directors at its meeting held on [date]. Effective until its next review, scheduled for [date], unless exceptionally amended by the Board.

1. General Qualitative Statement

[Company Name] conducts [briefly describe the principal activity] with the objective of [the company's strategic objective]. In pursuing these objectives, it takes risks consciously, on an informed basis, and within the limits approved by the Board of Directors.

The Company maintains an overall [conservative/moderate/aggressive — select] stance toward risk, prioritizing [priority objectives: solvency/growth/return/continuity/reputation] over [factors that may be traded off]. Risk-taking decisions are framed within the Three Lines Model and overseen by the Board's [Risk Committee].

2. Risk Appetite by Risk Category

The following five-level scale is used:

- Averse: no risks are accepted in this category except in exceptional circumstances approved by the Board.
- Minimal: clear preference for low-risk options. Only very low residual risks are assumed.
- Cautious: preference for safe options with low residual risk and limited return opportunity.
- Open: willingness to consider all options and choose the one with the greatest likelihood of success, taking risk into account.
- Hungry: willingness to consider innovative or higher-risk options that offer superior returns.

Category	LEVEL	SPECIFIC STATEMENT	METRIC / LIMIT
Strategic	[Open]	Accepts strategic investments with medium-term return horizon	Minimum ROI: [X]% over [Y] years
Financial — Liquidity	[Cautious]	Maintains coverage for stress scenarios	Liquidity ≥ [X] months
Financial — Credit	[Cautious]	Limited concentration by customer and sector	Client concentration: ≤ [X]%
Operational	[Minimal]	No material failures tolerated in critical processes	Operational losses: ≤ [X]% income
Compliance	[Averse]	Does not tolerate material breaches	[Zero] material sanctions
Reputational	[Averse]	Does not accept actions that harm reputation	[Zero] material events/year
Cyber	[Minimal]	Continued investment in cybersecurity	NIST maturity: level [X]

Category	LEVEL	SPECIFIC STATEMENT	METRIC / LIMIT
ESG	[Cautious]	Meets environmental and social commitments	ESG metrics by sector
Innovation	[Hungry]	Accepts investments that may not generate short-term return	Up to [X]% of the R&D budget

3. Tolerances and Escalation Thresholds

Three tolerance levels are established for each metric above:

- Green: within appetite. Normal management by the first line.
- Amber: near the limit. Notification to the CRO and CEO. Action plan defined.
- Red: exceeds appetite. Immediate escalation to the Risk Committee. If materiality warrants, escalation to the Board within [X] business days.

4. Effective Term and Review

This Statement will be reviewed at least annually and earlier if there are material changes in strategy, significant adverse events, relevant regulatory changes, or material corporate reorganizations. Amendments will be proposed by the Risk Committee and approved by the Board of Directors.

Annex II: Risk Matrix Template

The risk matrix is the operational tool that consolidates identified risks, their assessment, and handling plans. The following template is a recommended minimum structure that each company may expand according to its maturity.

The following scales are illustrative. Each company should calibrate the financial thresholds to its size and structure.

Probability Scale (example)

LEVEL	Description
1 — Rare	Probability < 5% within the time horizon considered. Very unlikely event.
2 — Unlikely	Probability > 5 and ≤ 25%. It could occur in certain circumstances.
3 — Possible	Probability > 25 and ≤ 50%. It could occur under normal circumstances.
4 — Likely	Probability > 50 and ≤ 75%. The event is likely to occur within the time horizon.
5 — Almost Certain	Probability > 75%. The event is expected to occur.

Impact Scale (example)

LEVEL	Description
1 — Insignificant	Financial impact < 0.1% of revenue; no reputational or regulatory effect.
2 — Minor	Financial impact > 0.1% and ≤ 1% of revenue; local, temporary reputational impact.
3 — Moderate	Financial impact > 1% and ≤ 5% of revenue; regional reputational impact; regulatory warning.
4 — Major	Financial impact > 5% and ≤ 15% of revenue; national reputational impact; regulatory sanction.
5 — Catastrophic	Financial impact > 15% of revenue; international reputational impact; business continuity crisis.

Matrix Template

FIELD	Description	EXAMPLE
Risk ID	Unique identifier	R-FIN-001
Category	Category by taxonomy	Financial — Credit
Risk name	Specific name	Main customer concentration
Description	Cause, event, consequence	Loss of the main client by...
risk owner	First-line owner	Sales Director
Inherent probability	Scale 1-5	3 — Possible
Inherent impact	Scale 1-5	4 — Major
Inherent level	Product P × I	12 — High
Existing controls	List of controls	Portfolio diversification; SLAs...
Residual probability	After controls	2 — Unlikely
Residual impact	After controls	3 — Moderate
Residual level	Product P × I residual	6 — Medium
Appetite	Category appetite level	Cautious
Status vs. appetite	Green / Amber / Red	Green
Associated KRIs	Monitoring metrics	Client concentration >X%
Handling plan	Actions, owner, deadline	Diversify by adding 5 new customers within 12 months
Last update	Date	[YYYY-MM-DD]
Next Revision	Scheduled date	[YYYY-MM-DD]

Annex III: Risk Governance RACI Matrix

The RACI matrix accurately distributes responsibilities for key activities of risk management framework. The conventions are:

R Responsible;

A Accountable;

C Consulted;

I Informed.

This matrix is a starting point: each company should adapt it to its organizational structure. In companies with a combined Audit and Risk Committee, the "Risk Committee" and "Internal Audit" columns should be adjusted accordingly. In companies without a formal CRO, CRO responsibilities fall temporarily to the CFO or another person designated by the Board. The critical requirement is that every activity have one **clearly identified accountable party (A).**

Activity	Board	Risk Committee	CEO	CRO	1st Line	Internal Audit
Approve the Policy	**A**	**R**	C	C	I	I
Approve the RAS	**A**	**R**	C	**R**	I	I
Define risk taxonomy	I	**A**	C	**R**	C	I
Identify material risks	I	C	**A**	**R**	**R**	C
Assess probability and impact	I	I	**A**	**R**	**R**	I
Define handling	I	C	**A**	C	**R**	I
Implement controls	I	I	**A**	C	**R**	I
Monitor KRIs	I	C	**A**	**R**	C	C
Quarterly report to the Committee	I	**A**	C	**R**	C	I
Annual report to the Board	**A**	**R**	C	**R**	I	I
Escalate material breaches	**A**	**R**	C	**R**	C	I
Approve breaches of appetite	**A**	**R**	C	C	I	I
Audit the framework	**A**	C	I	C	I	**R**
Approve audit plan	I	C	I	I	I	**R**
Provide risk training	I	C	**A**	**R**	C	I
Review the Policy annually	**A**	**R**	C	**R**	C	C

Sources

IDB Invest, “IDB Invest Corporate Governance Tool” (2024)

Corporate Governance Development Framework, “Corporate Governance Progression Matrix” (2024)

Good Governance Institute, “Board guidance on Risk Appetite” (2020)

IIA, “The IIA’s Three Lines Model” (2020)

Institute of Risk Management (IRM), “Risk Appetite and Tolerance — Guidance Paper” (2011)

OECD, “G20/OECD Principles of Corporate Governance” (2023)

PSOJ, “Navigating Corporate Governance” (2024)

UK Government, “Risk Appetite Guidance Note” (2021)

UK Government, “The Orange Book Management of Risk – Principles and Concepts” (2026)