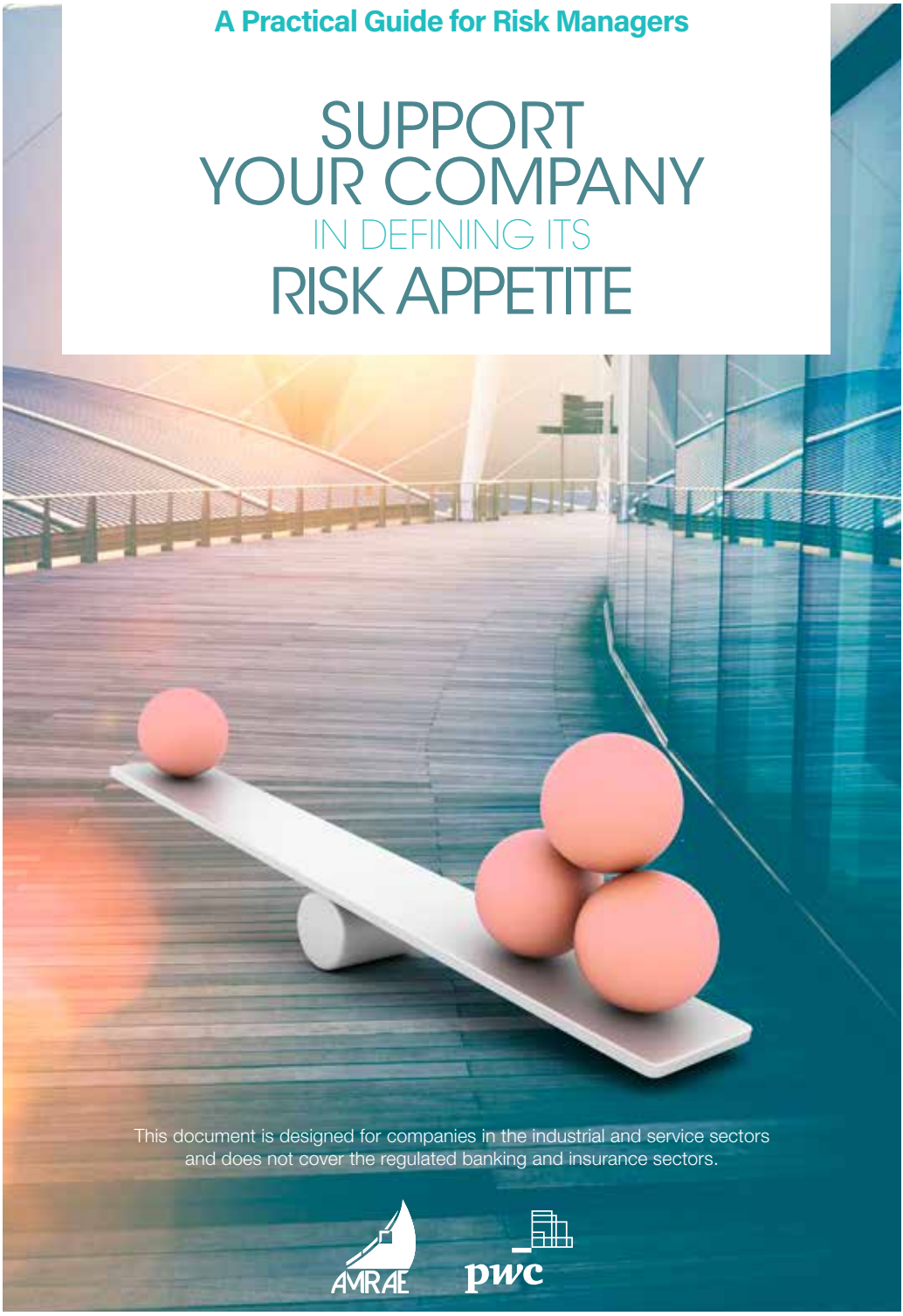
A Practical Guide for Risk Managers

SUPPORT YOUR COMPANY IN DEFINING ITS RISK APPETITE



This document is designed for companies in the industrial and service sectors and does not cover the regulated banking and insurance sectors.

AMRAE

pwc

AMRAE particularly thanks Françoise Bergé (PwC France and Maghreb), the members of the ERM 360° Commission of AMRAE (Stéphanie Canino, Winifrey Caudron, Sylvie Mallet, Philippe Noirot), as well as Laurent Magne for the preparation and drafting of this document, without forgetting Gérard Payen and Anne Piot d'Abzac for their proofreading, and Hélène Dubillot for the coordination of the publication.

About AMRAE

AMRAE (**A**ssociation pour le **M**anagement des **R**isques et des **A**ssurances de l'**E**ntreprise) is the professional association of reference for the risk and insurance professions in companies. It brings together more than 1,500 members from over 750 private and public organizations.

AMRAE supports these organizations in achieving their strategic and operational objectives to enable them to improve their performance and control their risks.

Risk management is a virtuous process that protects the company, its employees and partners, including insurers, and thus the economy as a whole.

AMRAE the Association brings together the major actors of the lines of control (Risk Management, internal control and audit, insurance, legal ethics...).

Through its scientific committees, its publications and its numerous events, AMRAE produces for these experts the content that feeds their skills, their development in their profession and their contribution to the success of the of the company's strategy.

With AMRAE Formation, it meets their needs for professional development development needs adapted to the evolution of organizations, by providing high-level by providing high-level training courses leading to certification.

AMRAE Les Rencontres organizes the leading annual conference for the risk and insurance professions (more than 3,000 delegates in 2020). These three days are the essential meeting place for all those involved in risk management and its financing.

About PwC France and Maghreb

In France and the Maghreb, PwC provides consulting and audit services, as well as tax and legal expertise, with the strategic ambition of being the benchmark in trust and business transformation industry-wide. More than 6,000 people work in PwC's entities in France and the Maghreb, sharing their expertise across an international network of more than 328,000 people in 152 countries. For more information, visit www.pwc.fr.

SUMMARY

Risk-taking is inherent to a company in its pursuit of value creation. However, due to the radical transformation of some "traditional" business models, increased digitalization of the economy, development of new technologies, multiplication of regulations, geopolitical uncertainties, changes in society, or the challenges of climate change, corporate risks are changing rapidly. Thus, it appears essential to improve the guidelines for risk-taking. The organization must be able to understand risks related to opportunities to create value (financial or not).

It is essential for the company to align with its internal stakeholders (employees and corporate governance) on the risk-taking strategy, and to communicate on this subject to its external stakeholders (customers, investors, and authorities).[1,2]

Each company[3] approaches its risk-taking according to its vision, mission or purpose, strategy, culture, resources, and the context in which it operates, especially the regulatory environment. It also defines the risks it is prepared to take, that can be defined as, the **risk appetite**[4], in accordance with what its shareholders and other stakeholders expect or can afford.

Risk appetite differs from one company to another and is also likely to change over time as a result of changes in the company, or under the influence of external factors such as changes in competition and technology, or a period of economic recession.

In the banking and insurance sectors, regulation has addressed the subject and requires the deployment of a Risk Appetite Framework aimed at defining, disseminating, and monitoring the implementation of Risk Appetite, which it defines as "the level and type of risk that an institution can and wishes to assume in its exposures and activities, taking into account its operational objectives and obligations".[5,6]

This regulatory framework does not currently exist in other sectors of activity; however, regulations can define limits for certain risks that are imposed on the companies concerned.[7]

When defining their operational risk appetite, banks face the same challenges as companies in other sectors, including:

- **How to express the appetite for operational risk at the top of the organization,** considering the multiple dimensions of this risk, the absence of robust measurement methods and the fact that the management of these risks is often decentralized throughout the organization?
- **How can operational risk appetite be taken into account in decision making,** given the difficulty of linking an overall risk appetite statement to performance indicators or more granular risks?

What is risk appetite for a company? How is it defined and communicated? How can the risk manager support his company in defining and communicating its risk appetite?

AMRAE set up a think tank to answer these questions. This document, which is the result of the group's work, aims to provide risk managers with useful elements for formulating risk appetite, disseminating it within the company, and communicating it. It is divided into two parts. The first part considers the definitions and principles, while the second describes practices illustrated by examples of approaches implemented by certain companies, in particular to initiate discussion within the Board. It is aimed at risk managers in companies of all sizes and sectors[8] and their internal stakeholders, including managers of the three lines of defense[9], directors and administrators. It is aligned with the work of the "Institut Français des Administrateurs" (IFA), which published "The role of the Board in determining the Risk Appetite"[10] in January 2016. It complements this work by putting into perspective the contribution of the risk manager on this topic.

1. AMF practice notes on questions that may arise regarding the application of Regulation (EU) 2017/1129 (Prospectus Regulation) and in particular on the application of Article 16 on risk factors; ESMA Guidelines on risk factors under the Prospectus Regulation, ESMA31-62-1217, March 2019.
2. A company's internal stakeholders include its managers, employees, unions and shareholders. Its external stakeholders are, for example, its customers, suppliers, supervisory authorities, rating agencies and, more generally, civil society.
3. The term Enterprise in this document covers all private, public and semi-public organizations, regardless of their size.
4. AMRAE uses the term Risk Appetite, although some French publications use the term "appétit aux risques" and others use the English term Risk Appetite without translating it.
5. Internal Control Order of November 3, 2014 (transposition of CRD IV) which frames the definition of risks and limits that are integrated into the appetite framework.
6. The Risk Appetite is formulated through the Risk Appetite Statement, making the link with the strategy (short and long term), and highlighting the internal limits for each type of risk.
7. Exposure limits for dangerous materials, for example.
8. It does not deal with the case mentioned earlier in the text of companies in sectors such as banking and insurance, for which regulations provide a framework for risk appetite practices.
9. Three lines of control for better performance, AMRAE IFACI, 2013
10. In the following, the terms Board or Board of Directors are used interchangeably and refer to the governance bodies in different organizational schemes, such as an organization with a management board and a supervisory board.

1 What is Risk appetite ?

Risk appetite determines the company's risk management strategy and thus facilitates risk-taking in the context of decision-making processes, for example related to the definition of the strategic plan, the validation of investments, and the negotiation and signing of commercial contracts. It also helps limit cognitive bias in the decision-making process, as it allows better alignment with the criteria.

1.1 Definitions

Aside from the banking regulator's definition, there are numerous other definitions of risk appetite in literature. Those used by the major frameworks and the IFA are covered in the following sections.

Definition used by COSO[11] in its framework published in 2017 "Enterprise risk management: an approach integrated with strategy and performance"

Risk Appetite is defined as **"the types and amount of risk, on a broad level, an organization is willing to accept in its pursuit of value. The first expression of risk appetite is an entity's mission and vision".**

11. COSO (Committee of Sponsoring Organizations of the Treadway Commission) is a committee of several American professional associations such as the Institute of Internal Auditors, which aims to establish standards for risk management, internal control and fraud prevention.

ENTERPRISE RISK MANAGEMENT

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

One of the twenty principles developed by COSO (Principle 7) deals with Risk Appetite and describes the recommended good practices:

- The company defines its Risk Appetite in relation to its culture and strategy.
- To do this, it relies on a range of techniques such as workshops, historical analysis of performance objectives vs. results, and modeling of risk scenarios.
- The Risk Appetite is formulated in general terms by the nature of risks (unacceptable risks) or quantitatively (amount of risk).
- Management fosters a corporate culture that makes them accountable for taking risk, and risk appetite, into consideration in decision-making.

1

In 2020, COSO published a statement on the contribution of risk appetite for companies that must manage their activities in a troubled geopolitical and socio-economic environment.[12]

Definition used by the AFNOR in the ISO 31000 standard "Risk management - Guidelines"

"Risk appetite policy consists **of the formalization by the governing bodies of expectations and limits on risk-taking.** This formalization must be the result of discussions in which the points of view of the management bodies and, more generally, of the stakeholders have been taken into account, or at the very least have been heard. The risk appetite policy is the final document that sets out the organization's vision of risk-taking. It is binding and applies to everyone."

Definition used by the IFA in its 2016 work

Risk Appetite is **"the definition of the type and level of risk that a company is willing to accept regarding its strategy. This "desired" level of risk is the balance between the potential benefits of taking a risk (an innovation, an investment, etc.) and the threats inherent in all changes".**

1.2 Position of AMRAE

Risk appetite is a key notion that accompanies - or should accompany - any decision-making process, in order to help clarify it, whatever its level (strategic or operational) and its domain (operations, human resources, finance, information technology, marketing, legal, communication, etc.). The company must work on the balance between the expected value of a decision, and the level of risk that it generates, or that it is willing to take in order to implement it.

Formulating a company's risk appetite is a complex exercise. First, the company's values, resources, culture, strategy and regulatory environment must be taken into account. It is also necessary to manage the balance between the different points of view expressed in a management team. Finally, without compromising the leadership of the management team, it is sometimes useful to take into account the expectations of certain stakeholders, who may have different views

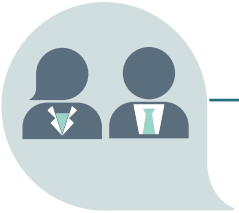
12. Risk Appetite – Critical to Success, Using Risk Appetite to Thrive in a Changing World, COSO, 2020

and analyses of the company's strategy and objectives. This approach is supplemented for certain areas of risk to which the company is exposed by limits laid down by regulation.

The company must also constantly adapt to new threats, some of which are linked to opportunities. This is the case, for example, for risks linked to cyber security and opportunities linked to digitalization. Thus, in alignment with its stakeholders, the company must be able to specify its appetite in relation with these risks.

Risk appetite is also expressed in the company's choices in terms of insurance coverage and, in particular, the choice between low premium and high deductible, or high premium and low deductible. In the same way, the historical crises that the company may have experienced and the way in which they were handled and managed impact its level of risk appetite.

Senior management is responsible for formulating the company's risk appetite, setting limits for the areas of risk for which this is relevant and obtaining approval from the Board of Directors[13]. The Board of Directors, in conjunction with senior management, must ensure that the proposed risk appetite is consistent with the company's values, strategy and resources.

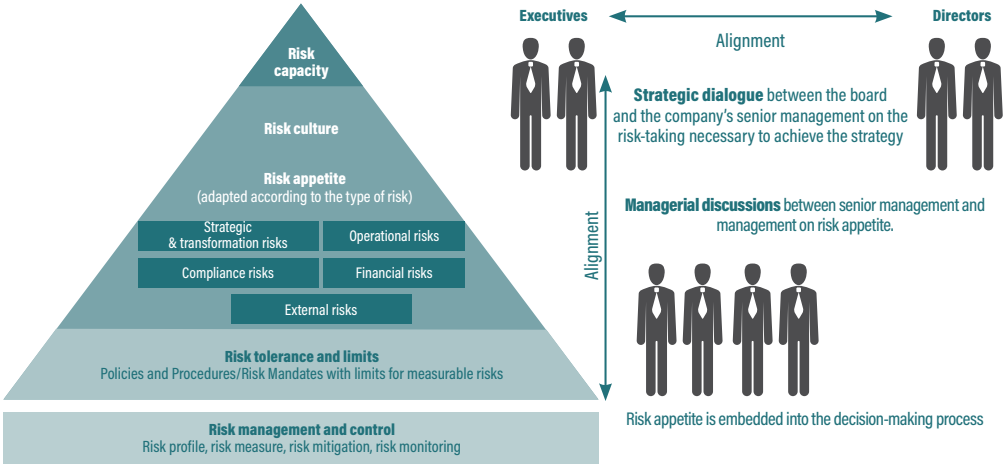


The Risk manager is involved in this process. He provides technical and methodological support by communicating information on industry practices, leading discussions on risk-taking within the company, and assisting in the formulation of risk appetite, the definition of limits and discussions with the Board of Directors. He supports the communication of risk appetite in the context of its risk analyses and in the decision-making bodies in which he participates.

13. Or a committee authorized by the Board for that purpose.

1.3 Risk management components associated with risk appetite

Risk appetite must be addressed in conjunction with several other components of risk management, represented in the illustration below.

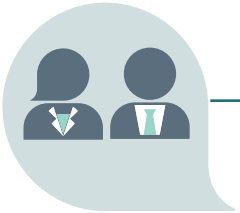


The company's risk capacity

The level of risk that the company can bear is determined by its financial, intangible and human resources, the regulatory and operational restrictions (e.g., technical infrastructure, expertise, etc.) that apply to it, and the commitments it has made to its stakeholders.

Risk capacity is the maximum level of risk that the company can bear over a given period without compromising its long-term viability. Risk appetite is established taking into account this capacity.

Discussions between the Board of Directors and senior management on the company's risk capacity are important as the subject is strategic. The Board may consider that management is not taking enough risk regarding the company's capacity and its expected value creation, or on the contrary, that it is taking too much.



The Risk manager helps the company to ensure that the risks to which it is exposed do not exceed its risk capacity by developing risk scenarios ("worst case" scenarios that remain realistic) and risk accumulation scenarios. In order to achieve this, actuarial studies can be used.

The company's risk culture

The company's culture influences risk-taking. It determines how all employees (executives, managers, and staff) perceive, understand, exchange and act on the risks faced by the company.

It also influences the perception of risk. Most of the time, risk is perceived as a threat that the company is afraid of. However, risk-taking is inseparable from the act of doing business and is necessary for the realization of the company's strategy. Thus, the differences in risk perception are often highlighted between so called "mature" companies which develop a risk perception oriented towards the threat, and "start-ups" which, generally, tend to focus on opportunities.

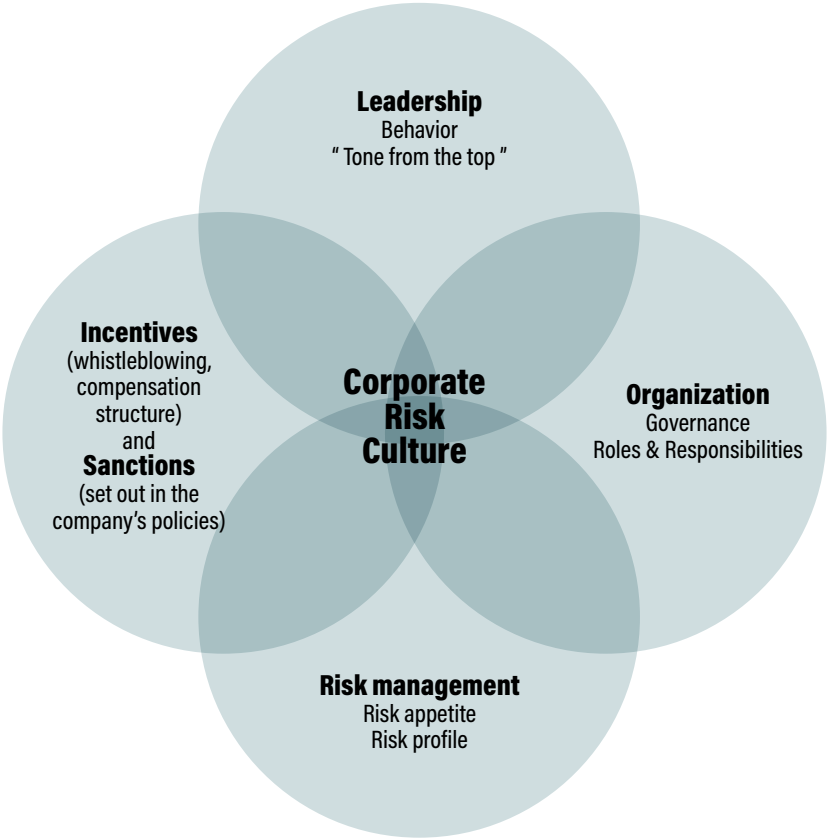
The aim of risk appetite is precisely to deal with this apparent contradiction: the idea is to manage risk-taking through a shared reflection on the risks that the company is prepared to take in different situations.[14] The company may decide to take a risk if it offers opportunities (for example, an innovation or an acquisition), or if it is able to react to its occurrence or to absorb its impacts. The risk is sometimes inherent to its economic or operational model (this is for example the case for industries dealing with hazardous products), or necessary for its survival (redeployment of its activities in the event of a disruption in its core business for example). On the other side, some risks may be considered as "unacceptable". These include risks that affect people and the environment, or that are related to the violation of ethical rules and laws.

Recent reviews of several corporate governance[15] codes emphasize the role of the Board in defining, evaluating, and monitoring corporate culture.

The main elements of a risk culture include:

- exemplary behavior at the highest level of the organization,
- an environment open to discussion,
- the systematic analysis of crises or near-crises experienced by the company[16] to learn from them,
- a shared awareness of the risks to which the company is exposed.

14. Some articles or statements introduce the notions of risks feared vs. risks taken, or of risks wanted vs. risks suffered.
15. For example: the UK Corporate Governance Code which, like other codes, prescribes the evaluation of the corporate culture by the board, Japan's Corporate Governance Code or the Dutch Corporate Governance Code.
16. Examining the crises experienced by other companies also provides valuable lessons for the company.



The Risk manager contributes, along with the other functions in the second line of defense, to the definition and diffusion of behaviors adapted to the company's culture and risk appetite. He collaborates with internal audit to assess the alignment between actual and expected behaviors, and to ensure that the necessary measures are taken to reduce any gaps.

Risk tolerance and limits set by the control environment

Risk tolerance reflects, for measurable risks, a certain degree of flexibility around a target value that derives from the framework set by risk appetite. Operating within the limits of the risk tolerance ensures that the company acts consistently vis a vis its risk appetite. Thus, a company that has defined the maximum unavailability rate of its critical information systems at 0.01% can tolerate a 20% deviation from this rate for the subsidiaries it integrates.

The difference between risk appetite and risk tolerance is illustrated in particular by risks that are considered unacceptable by the company, such as health, safety and corruption risks. As "zero" risk does not exist, unless the activity is eliminated at its origin, risk tolerance allows us to recognize the fact that events may occur despite the prevention measures in place. The occurrence of a risk must therefore be systematically accompanied by an analysis of the causes, treatment measures and, if necessary, sanctions.

These elements are documented in the policies, procedures or risk mandates that constitute the company's control environment. As an example, for financial risks, when possible indicators are put in place to monitor compliance with limits.

The company's risk profile

The company's risk profile is generally established using risk mapping, an exercise most often coordinated by the risk manager. It reflects the risks to which the company is exposed, identified at the time the mapping is made.

Risk mapping is based on a scale of impacts specific to the company which, when the company has not yet defined its risk appetite, constitutes an indicator of this appetite. This impact scale, which is often proposed by the risk manager and then validated by senior management and the governance bodies, determines the thresholds beyond which the consequences of a risk are considered critical and/or must be addressed.

Once the company has defined its risk appetite, the risk manager proposes a scale of impacts consistent with it.

Actions to strengthen risk mitigation are decided when the criticality[17] of a risk is judged to be too high and must be reduced to a target level (the maximum level to which the company wishes to see the risk evolve, by a given deadline). This target, validated by management, directly reflects the company's risk appetite for risks of this nature.

17. The criticality of a risk corresponds to the intersection of its probability of occurrence and its impact.

Some critical risks that are necessary to achieve the company's strategy will be accepted even though they remain high despite the measures taken, even if these measures are - and must be - reinforced. One example is the risk linked to cybercrime, an external risk for which the company does not have all the levers of control, a corollary of the current strategies of digitalization of processes or offers.

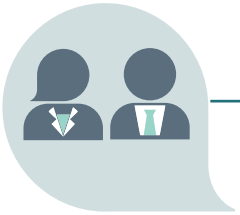
Finally, the company must monitor its exposure to risks and the implementation of the risk control measures it has decided to implement.

1.4 The main characteristics of risk appetite

Risk appetite is, by definition, aligned with the company's values and strategy

The company's values and commitments, for example in terms of health and safety, workplace well-being, ethics or inclusion, determine the company's risk appetite in certain areas.

Moreover, when senior management describe the guidelines chosen and the means implemented by the company to achieve its strategic objectives, they must also define and communicate the level of risk that the company is willing to accept as part of this strategy. Thus, to continue with the example of the risk related to cybercrime, the strategy of digitalization of the company's products or activities implies increasing the exposure to the "cyber" threat. When defining its strategy, the company sets market share and margin objectives for new products or effectiveness objectives for its activities. It must also determine its risk appetite so that appropriate means of prevention, detection and management of events are deployed.



The Risk manager contributes to the formulation of risk appetite in the scope of governance and strategic committees. Then, he ensures through the decision-making bodies in which he participates, that the discussions on the balance between the risks taken and the opportunities expected on each decision are in line with the risk appetite formulated in the context of the strategy.

1

Risk appetite takes into account stakeholder expectations

The company's internal and external stakeholders express their perception of risks and their expectations in terms of risk management in various ways.

Thus, regarding internal stakeholders:

- Discussions at Board meetings (for example, on risk mapping or on operations that the company submits to the Board for approval) and exchanges during strategy seminars enable administrators to express themselves on their risk appetite. This is done through their expectations in terms of value creation, their perception of threats to the company's business (such as technological disruptions or risks to key personnel) and their expectations in terms of prevention of certain risks such as fraud or corruption.
- Employee surveys and discussions at social and economic committees with employee representatives, provide an insight into their perception of certain risks and their expectations in terms of risk prevention.

For external stakeholders, companies often set up monitoring systems based on methods such as customer surveys, materiality studies or stakeholder committees as part of their CSR (Corporate Social Responsibility) approach in order to understand their perception of the acceptability of risks.

Furthermore, companies share rules, commitments and practices with their service providers and suppliers, in particular to take the necessary measures to control risks related to aspects such as respect for human rights, health and safety in the workplace, compliance with labor laws, respect for climate and environmental requirements, and the prevention of corruption.

When formulating its risk appetite, the company takes into account all the elements discussed above. It ensures global consistency between the company's strategy, values, culture, commitments and achievements. However, this ability to ensure consistency is now an expectation of both internal and external stakeholders. In the long term, companies that communicate their risk appetite will strengthen the confidence of their stakeholders.

Risk appetite is generally expressed in qualitative terms. For some risk categories, the expression of risk appetite is accompanied by a quantified target.

For example, regarding the development of new activities or new products within the framework of the company's strategic plan, risk appetite is expressed quantitatively in terms of acceptable financial losses in relation to expected gains and the company's risk capacity.

For financial risks such as exchange rate risks, financial market risks or commodity market risks, risk appetite is also expressed quantitatively in terms of acceptable financial losses in relation to expected gains, hedging costs and the company's risk capacity.

In other areas, the impact of risks cannot be measured directly in terms of financial losses but can nevertheless be quantified. This is the case, for example, with the risk of product below quality, which can be expressed in terms of a rejection rate. Risk appetite is then determined with regard to the company's strategy, the quality requirements of customers, the desired level of customer satisfaction, the cost of poor quality and the cost of improvement measures. It is translated into quality level objectives.

For risks difficult to quantify, such as risks related to the unavailability of resources or functions essential to the survival of the entity, the company can formulate its risk appetite by including in its policies a requirement for business continuity, including prioritization of access to resources (for example a succession plan or a "key person" insurance plan).

Finally, as mentioned above, for risks that have an impact on the health, safety and well-being of employees or populations, or on the environment or corruption, companies generally express their unacceptability and therefore commit themselves to implementing methods of protection in line with best practices.

2 Formulate, spread and communicate risk appetite

Risk appetite defines the level of risk taken by the company for each of its central decisions in relation to the expected benefits, for instance:

- the launch of a new product,
- the development of a new market (new segment or new area),
- a commercial offer (and its contractualization),
- the launch of a business transformation project,
- an external acquisition project.

Risk appetite is built, spread and expressed within the company, in the following ways:

- exchanges and decisions within the governance bodies,
- discussions and decisions within committees (investment committee, new products committee, offers committee, steering committees for transformation projects, ethics committee, etc.),
- discussions and decisions on the scope of global risk mapping (for example, at the company level, at the entity level or at the process level) and targeted risk analyses (industrial risks, risks related to financial markets, corruption risks, fraud risks, psycho-social risks, etc.),
- the control environment (delegations of powers, delegations of authority or signature, policies and procedures),
- exchanges and decisions in the context of activity reviewing,
- the attitude of local management and executives, which may encourage, or in some cases hinder, the expression of risks and the discussion of treatment strategies.

It is also influenced by individual and collective cognitive biases. Indeed, as the IFA report emphasizes, behavioral studies conducted on cognitive biases in decision-making, particularly when it involves risks (for example, during investment committees or new product launches), show that individuals are reluctant to take identified risks, while being structurally "optimistic" or confident in the future. Companies tend to amplify these behaviors, notably because of an asymmetry between risk-taking and expected gain, and sometimes because of a lack of individual responsibility in favor of consensus.

We can therefore see that the actual risk appetite that exists in a company may not correspond to the one that would have been desired by the Board of Directors and may not be adapted to the company's risk capacity. The formulation of a formal risk appetite makes it possible to avoid potential discrepancies and to better detect them, and promotes the structural alignment of the company's decisions.

2

2.1 Roles and responsibilities in risk appetite formulation and dissemination

Within the framework of the tasks assigned to it by the Commercial Code[18], the Board of Directors establishes the company's purpose and defines its strategy on the basis of proposals from the company's senior management. In this respect, it is responsible for formulating the risk appetite and the framework within which the senior management executes the strategy. In addition, as part of the Audit Committee's task of monitoring the effectiveness of risk management and internal control systems, and in particular through its review of risk mapping, the Board ensures that the company's risk profile is consistent with its risk appetite.

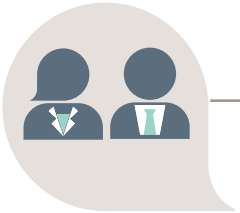
Senior management defines the framework (delegations of authority, policies, commitment authorizations, decision-making committees) within which decisions are made inside the company. In this respect, it ensures that this framework is consistent with risk appetite. It also contributes to the dissemination and compliance with risk appetite by highlighting the necessity for a balance between opportunities and risks in decisions.

The functional departments of the second line of defense define the rules that prevail in the control environment (policies and procedures) and monitor their application in the company.

The company's operational departments, the first line of defense, are responsible for managing the inherent risks of their activities and the risks resulting from the decisions they take in the context of risk appetite. To this end, they implement control operations in compliance with the rules set (first-level control). They integrate risk monitoring in the same way as performance monitoring in the management of their activities.

Internal audit, as a third line, ensures in its verification work that the control environment is consistent with the level of appetite formulated and is reflected in appropriate rules and indicators.

18. Articles of the commercial code 225-35 and following



The Risk manager supports senior management and the first and second line of defense. He provides the methodological framework and assists in formulating and disseminating risk appetite within the company. In conjunction with the other second line functions, he ensures second level control of compliance with the framework.

The Risk manager coordinates with the internal audit department (third line of defense), whose work provides an objective and independent assessment of the level of control over the risks covered by its audit plan. Failure of management to implement an important internal audit recommendation may reflect a lack of alignment with the organization's risk appetite.

2.2 Formulation of risk appetite

Based on the idea mentioned above, that entrepreneurship implies taking risks while respecting the company's values, and in an environment where human and material resources are by definition limited, a general formulation of risk appetite is emerging.

Thus, although the formulation of risk appetite is not today a common practice outside the banking and insurance sectors, all strategic or significant decisions of the company are a reflection of its risk appetite.

The formulation of risk appetite establishes a discussion between the Board and management on the limits within which senior management executes the strategy and thus contributes to the effectiveness of governance.

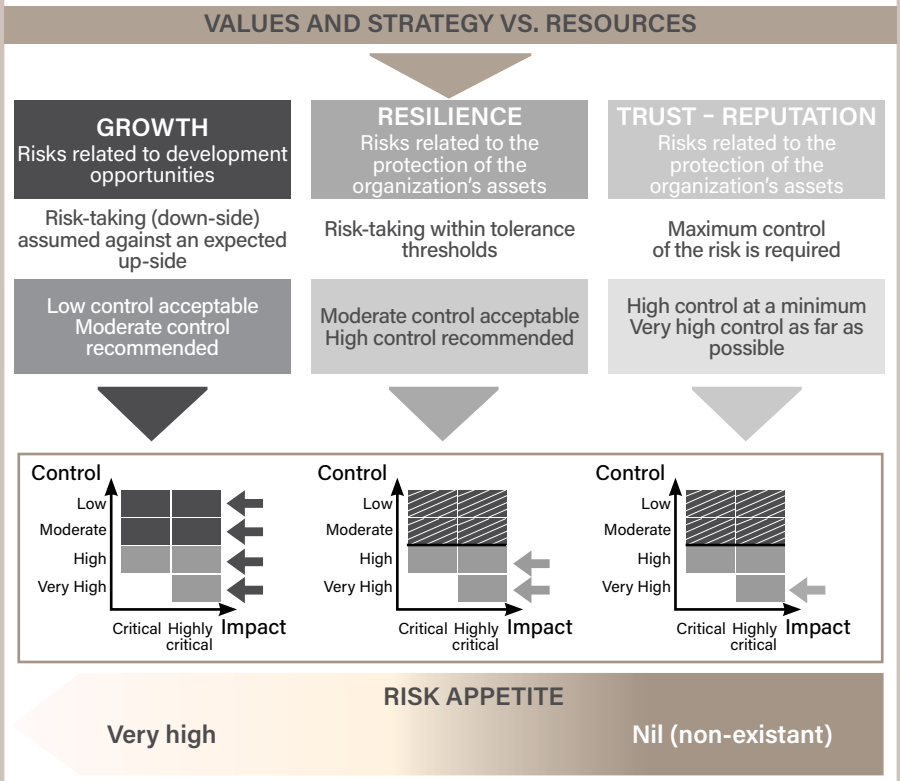
It also relies on Board discussions about the company's ability to face "reasonably pessimistic"[19], "black"[20] or "disruptive"[21] risk scenarios to ensure alignment between senior management and directors on the company's ability and willingness to take certain risks.

19. Scenario taking into account situations and events beyond the variations of parameters taken into account in the sensitivity studies of the median reference scenario.
20. A scenario that could have a catastrophic impact but whose probability of occurrence is very low. The increase in crises and the environmental risks that weigh on the activity of companies lead them to assess their resilience to such scenarios.
21. Scenario that takes into account a change in the competitive environment or a technological innovation that fundamentally the assumptions taken into account in the median reference scenario.

Illustration 1

In the example below, the risk manager proposes to formulate the risk appetite in relation to the desired level of control by distinguishing three types of risk:

- Risks related to development opportunities (launch of a new product or a new market, external growth, etc.);
- Risks related to the protection of major assets (partial or total shutdown of production) or impacting the efficiency of activities (failure of a supplier);
- Risks related to ethics, compliance or safety (employees and customers).



During the decision-making process, the three types of risk often coexist: the formulation of risk appetite makes it possible to structure the debate and the choices to be made.

Experience shows that while the formulation of risk appetite for reputational and resilience risks is generally agreed upon, the formulation of risk appetite for growth risks is often a subject of debate.

Illustration 2

The table below illustrates the possible types of formulation of risk appetite, overall appetite or by nature of risk.

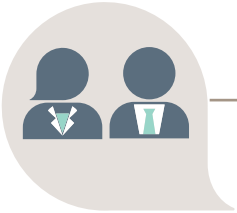
Types of formulation		Example
Qualitative	A qualitative formulation of risk appetite describes the company's risk culture, which risks are acceptable and why. It also links business and performance management to risk management.	▪ The company recognizes that some risks, while having potential undesirable impacts, cannot be avoided ▪ The company accepts risks for which the cost of treatment exceeds the estimated losses, or for which the estimated losses are within tolerance limits ▪ The company defines behaviors that are not tolerated, such as non-compliance with rules or environmental damage
Quantitative	A quantitative formulation is based on thresholds that indicate the level of risk tolerated.	▪ Level of performance, e.g., failure rate of critical systems ▪ Thresholds for company authorizations
Absolute	The formulation of the risk appetite sets the amount of acceptable risk expressed in €, volumes, deadline...	▪ Zero tolerance for non-compliance risks
Relative	The amount of acceptable risk is variable compared to a benchmark.	▪ Not suffering from greater losses than the competitors ▪ Tolerable losses are expressed as a proportion of operating income

Illustration 3

The illustration below provides an example of a scale to qualitatively express risk appetite, globally or by nature of risk.

The organization's risk appetite translates into actions to contain, control and limit risk

The organization's risk appetite translates into the level of tolerance to the occurrence of such events and the measures taken in case of their occurrence



The Risk Manager, in conjunction with the second line functions, and in particular the function in charge of strategy development, facilitates exchanges within the committees[22] and the Board in order to develop a formulation of risk appetite that is revisited if necessary, within the framework of the strategic cycles.

He coordinates the analysis of "black" and "disruptive" risk scenarios and leads discussions in the Board.

22. Risk committee if existing, management committee, executive committee or general management board.

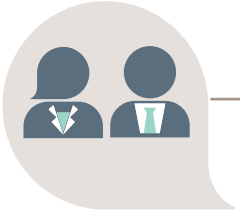
2.3 Spreading risk appetite within the company

Through its values and strategy, the company broadly disseminates elements of its risk appetite.

Furthermore, since the beginning of the 2000s, under the combined influence of the law[23] and professional codes and guides[24], companies have structured their governance and developed a control environment that provides a framework for decision making at all levels of the organization. For example:

- guidelines for the selection of suppliers,
- guidelines prohibiting any business activity with other third parties subject to economic sanctions,
- guidelines for occupational health and safety with targets and indicators that track the accident rate,
- guidelines for the availability of information systems with targets and indicators that track the failure rate,
- mandates for risks related to investments in financial markets (cash investments, for example) or risks related to the energy and commodities markets,
- guidelines on anti-corruption and anti-money laundering (see Sapin 2 law).

These guidelines and practices form a framework that transcribes the company's risk appetite and it is a vehicle for its dissemination.



The Risk manager, in conjunction with internal control and the other functions of the second line of defense, analyses the consistency of the procedural framework and the limits set, and reports to senior management and governance on any inconsistencies, the need for adjustments over time due to changes in internal or external factors, and any deficits. As part of its work, internal audit periodically assesses this consistency.

23. New Economic Regulations Act (NRE, 2001), Financial Security Act (LSF, 2003), Act of July 3, 2008 containing various provisions adapting company law to Community law (known as the "DDAC Act"), recommendations of the French Financial Markets Authority (AMF)
24. Afep-Medef Code of corporate governance for listed companies (updated in January 2020) as well as the numerous guides published by the IFA, IFACI and AMRAE

2

Risk appetite is also spread within the company through the expression of its values and commitments, which influence behavior.

Finally, discussions in the context of management dialogue (discussions with local management, discussions in business reviews) and in decision-making bodies (such as the bid committee or the investment committee) are the third pillar of the dissemination of risk appetite.

The result of the spread of risk appetite is a corporate culture where decisions are made taking into account the company's ability and willingness to take certain risks.

Are risk analyses carried out and taken into account in the development of the strategy or medium-term plans?

If so, are these analyses broken down into several scenarios? For example: a "reasonably pessimistic" scenario, a "black" scenario (or "worst case" scenario), and a "disruptive" scenario.

Do managers decide on the acceptability of major risks in relation to the company's risk capacity?

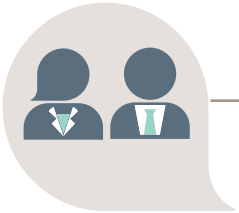
Are independent risk analyses provided to the decision-making bodies?

Is the risk/opportunity/financial capacity balance discussed at decision-making meetings?

Are risks treated with the necessary attention during business performance reviews?

Are deviations of indicators from acceptable limits made explicit in performance reviews?

Are risks a regular topic in senior management dialogue?



The Risk manager actively contributes to the spread of risk awareness within the company through exchanges with the three lines of control as part of their work (coordination of the risk mapping process, monitoring of emerging risks, analysis of disruption risks, etc.) and in the decision-making bodies in which they participate (project, investment and strategy committees, etc.). The Risk manager leads awareness and training sessions on risk management, which are the best way to spread risk culture. On these occasions, the Risk Manager contributes his knowledge of risk situations based on the history of the company in terms of strategic choices, decision-making and crisis management, as well as the analysis of emerging risks.

The risk manager provides risk analysis methods, is able to support some of them and can conduct analyses independently of management.

2.4 Monitoring compliance with the framework

Compliance with the rules and limits set by the control environment is monitored as part of internal control. A first level of control is ensured by the first line operational functions, and a second level by the second line functions. In some companies, the first and second lines' functions share dashboards containing the relevant risk indicators and monitor their evolution in relation to the limits set.

Different strategies can be considered in the case of limits being exceeded significantly and for lengthy periods of time, including:

- The company decides to accept the risk despite the fact that the limits have been exceeded, because it is a risk that is wanted and assumed. The limits must then be reviewed.
- The alert threshold has been reached, but the risk capacity has not yet been exceeded. A decision must be made as to whether to accept this level of risk in terms of the company's strategy or, on the contrary, to deal with it or transfer it, in order to return the limits set.
- The risk capacity has been exceeded: the company cannot bear this level of risk. A new strategy compatible with the company's risk capacity must then be defined.

In the case of a critical and lasting excess, the Board of Directors is informed of the deviations observed or envisaged, and of the intended strategies to return to the level of the defined risk appetite.

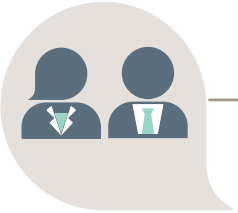
Internal audit ensures a periodic evaluation of the effectiveness of internal control.

2.5 Communicate about the company's risk appetite

Risk appetite is a company commitment. This is especially the case when a company mentions a target for workplace accidents, compliance or the environment.

Companies are being asked by the regulator or their external stakeholders to communicate more and more information on the risks they are exposed to and the means they use to manage them. Thus, even if companies outside the banking and insurance sectors are not currently obliged to communicate on their risk appetite, in the long term, this will be a way of reinforcing stakeholder confidence.

Each company determines the best way to communicate its risk appetite to its external stakeholders, taking into account confidentiality constraints in a competitive environment.



The Risk Manager participates in the development of the external risk management communication strategy and ensures that this communication is consistent with the vigilance required for communication on certain subjects, such as business confidentiality.

He monitors the implementation of the commitments made by the company in this area.

Some tips to start thinking about risk appetite in your company

The examples shared below illustrate practices initiated by some companies in starting to think about risk appetite. Some of them may be more or less relevant depending on your company's context. They can also be combined if necessary.

Example #1: Analysis of decision history

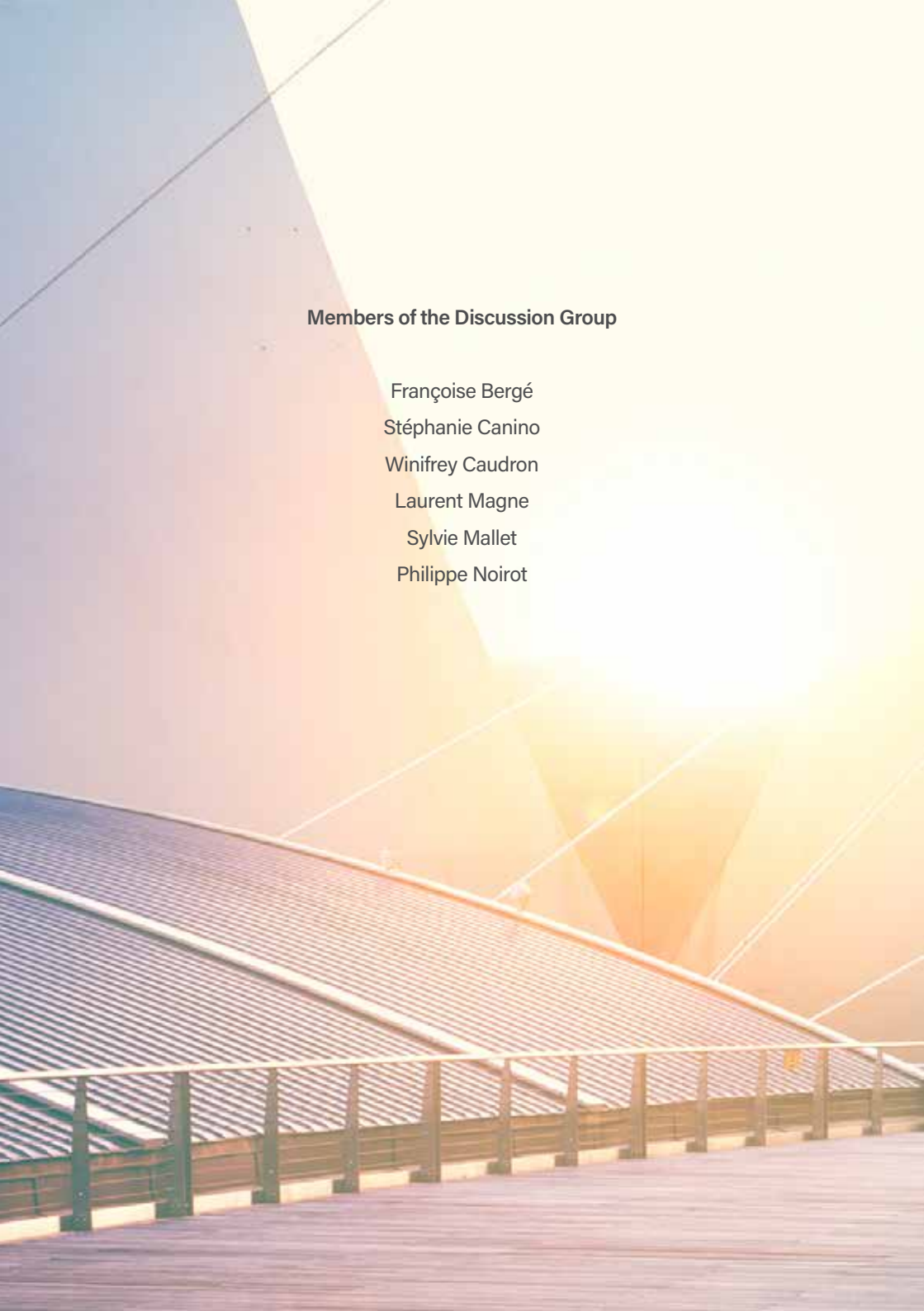
- Establish a list of the company's major decisions over the last few years (examples of source documents used - reports of Board of Directors, press releases);
- Analyze the evolution of the risk maps following the outputs of each of these decisions;
- Synthesize the lessons learned from the analysis in terms of risk appetite (ideally by identifying specificities by nature of risk);
- On this basis, animate some discussions with the Board for a common reflection on the formulation of risk appetite (possibly by nature of risk).

Example #2: Analysis of the control environment

- Identify the rules governing the delegation of authority and the decision-making processes (decision-making committees);
- Compare this with risk limits (for example, thresholds for employee exposure to dangerous situations in relation to regulatory thresholds), risk assessment thresholds and thresholds for activating crisis units;
- Drawing lessons in terms of risk appetite (ideally by identifying specificities by type of risk);
- On this basis, lead one or more discussions with the Board for a joint reflection on the formulation of risk appetite (possibly by type of risk).

Example #3: Definition of non-negotiable or unacceptable risks

- Analyze the internal and public positions of the company and its managers about risks (e.g., zero tolerance of corruption);
- Analyze the expression and evaluation of risks in the updates of the risk map and, if necessary, take into account the target level of risks;
- On this basis, propose to senior management and the Board a list of unacceptable risks, together with specific procedures for monitoring and taking action in the event of their occurrence.



Members of the Discussion Group

Françoise Bergé

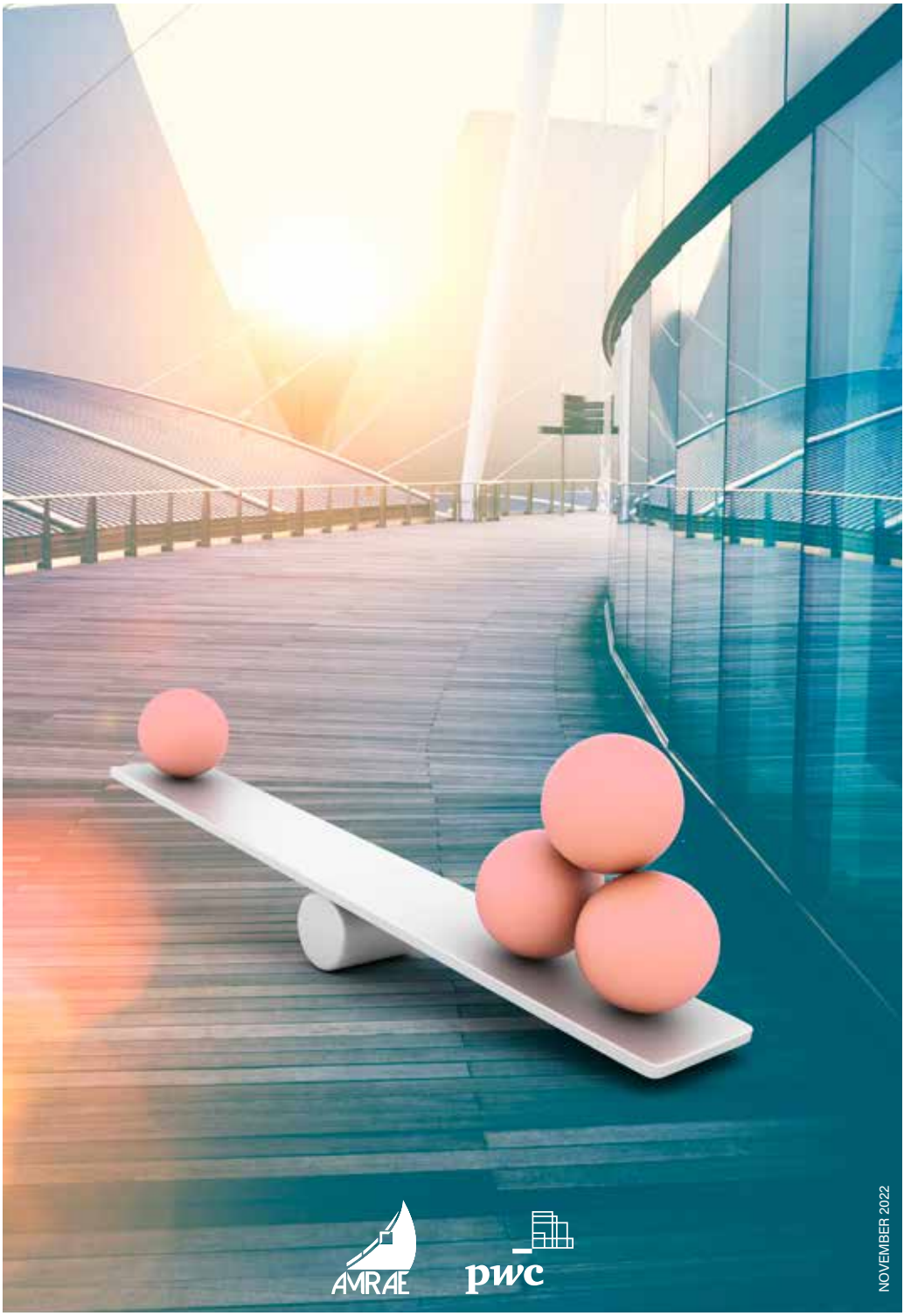
Stéphanie Canino

Winifrey Caudron

Laurent Magne

Sylvie Mallet

Philippe Noirot



AMRAE

pwc

NOVEMBER 2022