

Louvain School of Management

Emerging risks: An exploratory study of several case studies

How do companies, in the banking sector, build a process to consider emerging risks?

Author: Alexia Butaye
Supervisor: Loïc Decaux
Academic year 2020-2021
Thesis for the Master [120] in Management, professional focus
Daytime schedule (site of Louvain-la-Neuve)

Supervisor: Loïc Decaux

First of all, I would like to thank Loïc Decaux, my supervisor, for having guided me through the writing of this thesis.

I would also like to thank Argenta, Axa Bank, Belfius, Bpost Bank, Euroclear Bank, World Bank and the investment bank, for giving me their time and explaining their risk management process. Their input provided me with essential material that greatly contributed to the content of this thesis.

Finally, I thank Chapelle consulting, where I did my internship, who helped me to expand my knowledge in risk management and took the time to answer my questions.

*“We cannot predict the future, but we can study our environment and adapt accordingly
– the most successful firms are those able to adapt not through
magical foresight, but through constant observation and change”
(Chapelle, 2019)*

Table of content

Abbreviations meaning.....	iii
Important definitions in emerging risks	v
Explanation of risk management exercises	vi
Introduction	1
Part 1: Literature review	2
Chapter 1: Risk management	2
1. Emergence of enterprise risk management and definition.....	2
2. Enterprise risk management in the banking sector	4
Chapter 2: Emerging risks.....	5
1. Definition and historical perspective	5
3. Main emerging risks facing the banking sector	12
a. Major trends that influence emerging risks	14
4. Framework and regulation on the banking sector related to emerging risks	16
5. Stages in the consideration of emerging risks	19
a. Emerging risks identification	19
b. Emerging risks assessment	20
6. People involved in the process to analyse emerging risks.....	21
a. Chief Risk Officer and the risk management team.....	21
b. Board of Directors	23
c. Executive Committee.....	24
d. First line of defence	24
e. Internal audit and audit committee	25
f. Other teams involved	25
g. External consultants.....	26
h. Cognitive biases.....	26
Part 2: Empirical research	28
Chapter 1: Methodology.....	28
1. Subject of study and problematic	28
2. Research question and objectives	28
3. Research methodology.....	29
a. Methodology used for the interviews	29
□ Data collection	29
□ Data analysis	30
Chapter 2: Analysis of the emerging risk management process in the banking sector	31
1. How banks define the notion of emerging risks?	32
2. What are the main emerging risks and trends facing banks?.....	35
3. What are the reasons that emerging risks are taken into account by banks?	39
4. Who are the people involved in managing emerging risks?.....	41
5. At what stage in the management of emerging risks do banks use external consultants?	45
6. How do banks collect information needed to manage emerging risks?.....	47
7. How do banks process to consider emerging risks?	50
8. How is information on emerging risks shared within banks?.....	56
Corpus of good practices.....	62
1. Emerging risks identification.....	62
2. Emerging risks assessment	64
3. Emerging risks mitigation.....	69
4. Emerging risks monitoring	70
5. Emerging risks reporting	70
6. More generally.....	72

Conclusion.....	75
Further discussion.....	76
Limits faced.....	77
Bibliography.....	78
Appendices	90
Appendix 1	90
Appendix 2	92
Appendix 3.....	94
Appendix 4.....	95
Appendix 5.....	96
Appendix 6.....	97
Appendix 7.....	98
Appendix 8.....	99
Appendix 9.....	102
Appendix 10.....	103
Appendix 11.....	105
Appendix 12.....	106
Appendix 13.....	107
Appendix 14.....	109
Appendix 15.....	111
Appendix 16.....	114
Appendix 17.....	116
Appendix 18.....	117
Appendix 19.....	120
Appendix 20.....	123
Appendix 21.....	124
Appendix 22.....	128
Appendix 23.....	130
Appendix 24.....	132
Appendix 25.....	134
Appendix 26.....	136
Appendix 27.....	138
Appendix 28.....	140
Appendix 29.....	143

Abbreviations meaning

Abbreviations	Meaning
AML	Anti-money laundering
BIS	Bank for International Settlements
BofD	Board of Directors
CEB	Committee of European Banking Supervisors
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CFT	Combating the financing of terrorism
COO	Chief Operational Officer
COREP	Common Reporting Framework
CORO	Chief Operational Risk Officer
COSO	Committee of Sponsoring Organizations of the Treadway
CRD	Capital Requirements Directive
CRO	Chief Risk Officer
EBA	European Banking Authority
ECB	European Central Bank
EIB	European Investment Bank
ESG	Environmental, social and governmental
Exco	Executive Committee
IAA	International Actuarial Association
ICAAP	Internal Capital Adequacy Assessment
ICAEW	Institute of Chartered Accountants in England and Wales
IIA	Institute of Internal Auditors
ILAAP	Internal Liquidity Adequacy Assessment
IMF	International Monetary Fund
IRGC	International Risk Governance Council
ISO	International Organization for Standardization
KRI	Key Risk Indicator
Mgmt	Management
NBB	National Bank of Belgium

p&l	Profit and losses
RCSA	Risk and Control Self-Assessment
SREP	Supervisory Review and Evaluation Process
SSM	Single supervisory mechanism
UN	The United Nations
WEF	World Economic Forum

Important definitions in emerging risks

*According to my own words.

Type of risks	Definitions
External risks	Risks, such as pandemics or cyber-attacks, which the bank has no direct control or influence on them. And do not result from the bank's operational activities or strategy and for which preventive and corrective controls are necessary to mitigate them.
Financial risks	These risks include credit risks resulting from defaults; market risks resulting from declines in funds and investments; and liquidity risks resulting from the inability to realize cash and meet obligations.
Internal risks	Risks that depend directly on the bank's strategic choices and activities.
Operational risks	All non-financial risks resulting from people, processes, systems and external events, such as fraud risks, IT risks, climate risks, etc.

Explanation of risk management exercises

*According to my own words

Type of exercises	Definitions
Holistic approach	Risk management approach where risks are identified, analysed and/or managed collectively as a whole.
Key Risk Indicators	These measurements tools are used to assess risk exposure and compliance with the limitations in force within the bank. And thus, ensure that the risk appetite defined by the Board of Directors is respected.
Risk appetite	This concept refers to the degree of risk that the bank is willing to take. This is decided by the Board of Directors, on the advice of the risk team (the second line of defence). And can be established in economic amount, in social capital or any other measure depending on the type of risks.
Risk cartography	This exercise is carried out in the risk assessment phase where risks are assessed, in general, according to the probability of occurrence (on the y-axis) and the possible impact (on the x-axis). In this way, the bank can assess its level of exposure to risk, establish preventive controls and see which risks require greater vigilance.
Risk taxonomy	The risk taxonomy is a categorisation of risks, performed by the bank. It includes both financial and non-financial risks, or can go into more detail by identifying operational, liquidity, market and credit risks or other structures.
Scenario quantification	This step, included in the risk assessment

	phase, aims to identify the severity of each risk, both financial and non-financial, and the possible losses in monetary terms that these events may involve.
Silo approach	Risk management approach where risks are identified, analysed and/or managed individually.
Stress testing	Exercise that helps banks to see potential changes in variable which can affect its business continuity. As an example, for banks linked to the financial crisis of 2008 will be to evaluate the change of the housing prices compare to the previous years.

Introduction

On 13th and 14th July 2021, Belgium and Germany faced unprecedented flooding, costing hundreds of lives. Two weeks later, it was China's turn to be affected.

For more than two years, ecological disasters have followed one another, with devastating forest fires in Australia, California, Turkey and southern Italy, and pandemics bringing the world economy to a standstill, etc.

These climate risks are not the only ones to frighten, there is also the rise of cyber risks and the risk of a potential new financial crisis. Among the sectors fearing these events, qualified as emerging risks, we count the banking sector, which must adapt its strategy accordingly and avoid that these events materialize in big financial losses.

According to Giddens (1990 (as cited in Locklear, 2011, p.3)), emerging risks have their origins in today's global, dynamic and interconnected environment. However, responses and recommendations to manage these risks, from the regulator and supervisor, are slow in coming, as they are not able to define the degree of impact of these risks or when they will occur.

Therefore, the purpose of this thesis is to establish a corpus of best practices for the management of emerging risks in banks. To do this, I interviewed eight banks, large and small, commercial and investment, with the aim of understanding the deficit, or at least the lack of structuration, that persists in the management of these risks.

First, to understand the purpose of emerging risks and their management, a brief history of the notion of 'Enterprise Risk Management' from the literature will be given. In the next chapter, we will focus on emerging risks, what they are, why they are a real challenge for banks, and the regulations already in place, in this sector, to manage them. We will also look at the different people involved in their management.

Then, an analysis of the information collected during the interview of the banks will be carried out to finally arrive at the drafting of a corpus of good practices helping the banks to face the emerging risks as well as possible.

Part 1: Literature review

Chapter 1: Risk management

1. Emergence of enterprise risk management and definition

The concept of emerging risks cannot be seen directly without first understanding enterprise risk management (ERM) and a reminder of the definition of risk.

Indeed, risks are defined by the *International Organization for Standardization (ISO)* as “*the effect of uncertainties on objectives*” (ISO, 2018). Which must be taken into account in every decision made by the company and at all levels of the organisation, from the members of the Executive to the line of business that carries out the daily operations (Al-Farsi, 2020, p.87).

Indeed, although they are often seen as a threat, many authors also see them as opportunities to be considered, which is consistent with Aabo and al.’s view that define risk as” (...) *a strategic combination of vulnerability and opportunity*’ as well as ‘(...) *by its potential to threaten the achievement of business objectives (...)*’ (Aabo & al., 2005, p.62).

The notion of ERM first appeared in the decision-making process in the late 1940s and early 1950s to enable managers to consider the level of financial risks they were prepared to take. The concept is defined by the *Committee of Sponsoring Organizations of the Treadway Commission (COSO)* as “ (...) *a process, effected by an entity’s Board of Directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives*” (COSO, 2004, p.2) and emerged in the late 1990s for two reasons (Dickinson, 2001, p.360; Aebi, Sabato & Schmid, 2012, p.3213).

The first reason is the failure of large companies. We remember the *Enron* scandal in 2001 which led to the bankruptcy of the company, following a case of financial manipulation and fraud, to increase its stock market value, by taking advantage of the lack of regulation in its sector of activity. This led to the implementation of corporate governance for greater transparency and risk regulation. Moreover, following this scandal, the Chief Risks Officer (CRO) was given more responsibility for the implementation of better corporate governance (Liebenberg, 2003, p. 42).

The second reason was to avoid excessive losses thanks to the introduction of regulations requiring companies to respect a certain transparency and internal control rules. This is in line with Power's idea (2003, p.35) that the emergence of ERM is due to a need to control the risks

faced by companies. But the main reason for implementing ERM is “*improving the organisational performance*” (Al-Farsi, 2020, p.89) and to create value for the company's shareholders (Gordon, & al., 2009, p.302; Pagach and Warr, 2011, p.187).

Among the main features of ERM, there are “*formal written statement of risk appetite; having a senior manager assigned the responsibility of overseeing risk and risk management; and a formal risk management report submitted to board level regularly*” (Lundqvist, 2014, p.395). COSO (2004) and Holmquist (2019, p.48) have also developed their characteristics, I refer you to these authors for further information.

Various ERM frameworks were proposed in the literature search, the most important of which are those proposed by COSO in the United States of America and the internationally accepted ISO 31000, as well as that of the *International Risk Governance Council (IRGC)*, a Swiss-based think tank.

In addition to ISO, COSO and IRGC addressing a structure for all types of emerging risks, there are more specific organisations such as *iNtTeg-Risk (Early Recognition, Monitoring and Integrated Management of Emerging, New Technology related Risks)*. This organisation, created in 2008 by the *Seventh Framework Programme for Research and Technological Development (FP7)*, addresses risks related to the new technology industry on a European scale, focusing more on early signals of risk emergence and proposing slightly different steps in risk management than the frameworks proposed above. (Ashby & al., 2018; Jovanović & Löscher, 2013).

Although these organisations adopt their own definitions and structure, there is a link between the management of these risks and the company's objectives and strategy, with risks being measured (COSO, 2004). Indeed, the process of establishing ERM would institutionalise the implementation of standardised tools and methods and provide a strategy for effective risk management (Al-Farsi, 2020, p.88).

Until the financial crisis of 2008, financial risks were mainly considered in the financial sector. Following the crisis, the *Basel Committee*, also known as the *Committee on Banking Regulations and Supervisory Practices*, adapted its regulations by introducing “*(...) operational risks in addition to credit and market risks as part of the financial institutions' capital adequacy determinations*” (Basel, 2003 (as cited in Pagach & Warr, 2011, p.188)). Since then, operational risks have been included in the risk taxonomy.

Moreover, with the implementation of ERM, risks are no longer identified and analysed individually, as a silo approach which was a deficit approach in the ability to analyse changes in the external environment (Jovanović & Löscher, 2013). But now, a more global approach, called

the holistic approach is used, that takes into account the interdependent relationships between these risks (Aebi et al., 2012, p.3213; Al-Farsi, 2020, p.88; Gordon & al., 2009, p.301; Liebenberg, 2003, p.40; Pagach & Warr, 2011, p.187).

In addition to the consideration of non-financial risks, the crisis also led to the creation of a risk management committee and increased responsibilities of the Board of Directors (BofD) (McShane & al., 2011). Besides, greater transparency is required from companies, by shareholders and regulators, in their reporting on how risks in general are managed (Paape and Speklé, 2012).

Many scholars, although a debate continues to exist among the scientific community on this statement, have highlighted the implementation of ERM within banks, with the hiring of CROs whose responsibilities will grow over time as we will see in the section dedicated to this function (Al-Farsi, 2019, p.89).

Although the role that ERM has played in addressing emerging risks has been clarified so far, there remains a particular gap to be filled. Indeed, according to Ashby & al. (2018, p.3), ERM does not take sufficiently into consideration the lack of information regarding emerging risks. The authors add that the ERM is mainly based on historical knowledge and known information. Nevertheless, emerging risks are risks that are often uncertain or whose impact and probability of occurrence cannot be clearly defined due to the lack of information on these. Although they may have occurred in the past but remain emerging due to their evolution in the environment.

We will see, in the next subsection, how the concept of ERM is applicable to the banking sector. As well as how this framework is an essential structure for banks to deal with day-to-day risks but also with emerging risks.

2. Enterprise risk management in the banking sector

Bank, defined by Diamond and Rajan as “*an intermediary between agents who needs to borrow and those who are willing to lend or invest*” (Diamond & Rajan, 2001 (as cited in Nöth-Zahn, 2017, p. 9)), are subject to numerous regulations and guidelines, as we will see in the next chapter. Among the supervisors of this sector is the *Basel Committee* which has contributed to the development of ERM in financial firms (Pagach and Warr, 2011, p.186).

Mikes adds that “*the Basel Committee, leading the reform of banking supervision, endorsed enterprise risk management as an umbrella notion that can accommodate the techniques required for bank capital adequacy calculation (...)*” (Mikes, 2009, p.19).

Before developing an understanding of the importance of a risk management structure, which was precipitated after the 2008 financial crisis, it is important to remind that banks operate in a highly

regulated environment, subject to new and uncertain trends such as the consideration of climate risks or the emergence of new technologies, for which the *Basel Committee*, tends to provide to banks additional information and a regulatory structure, such as “(...) *risk assessment, capital needs planning, enhanced risk disclosure and increased governance responsibilities*” (Mikes, 2008, p.2).

Chapter 2: Emerging risks

1. Definition and historical perspective

Previously, we saw that the term ‘risk’ was defined according to two criteria: uncertainty and impact on objectives (ISO, 2018). In his work, Aven (2012, p. 42) analyses the different definitions of risk that exist. According to the author, a risk can also be defined as “*Risk = Consequences/damage/severity of these + Uncertainty* and the consequences refer to both positive (opportunities) and negative (threats) effects for the company.

It is important to clarify at the outset the definition of 'risk' used in this work, as there are a multitude of definitions put forward and analysed by Aven (2012)¹. But laying the groundwork on these two definitions provides a subjective perspective around which the definition of emerging risks and its characteristics will be established and analysed. Especially as Aven (2012, p.42) says that the perspective of the notion of 'risk' chosen has an influence on the way risk is analysed and influences decision making.

Besides, Aven and Flage propose three perspectives to identify the interpretation to be given to the notion of emerging risks. The first concerns “*that risk is an event*”; the second one is “*that risk is a combination of possible scenarios and their associated consequences and probabilities*” and the last one is about “*that risk is the combination of future events, the consequence of these and the associated uncertainties*” (Aven & Flage, 2015, p.62).

As for the term 'emerging', it is defined by the *IRGC* as “*a new or a familiar risk that becomes apparent in new or unfamiliar conditions*” (IRGC, 2010, p.5) or by Aven and Flage “*as newly created or noticed and growing in strength or popularity: becoming widely known or established*” (Aven & Flage, 2015, p.61).

¹ I refer you to his article entitled: *The risk concept—historical and recent development trends* (2012) for more information.

Regarding Jovanović and Löscher, the notion of emergence, derived from the term ‘emerging risks’, is only a contributing factor to the uncertain nature that influences the achievement of the objectives. In other words, they explain this term “*as the act or an instance of emerging or the act of becoming known or coming into view: the act of emerging*” (Jovanović & Löscher, 2013). Once the risk has materialized, and is subject to new regulations, or once the probability of it occurring is zero, it is considered known according to these authors.

Another distinction between emerging risks and other risks is that the former is difficult to quantify using traditional risk management techniques (Allan et al., 2012, p.179). A table comparing the definitions, characteristics, and main challenges between emerging risks and familiar risks is provided in appendix 1.

Regarding the term ‘new’, it refers to the fact that the risk did not exist in the past, but as a result of a change in the environment, such as a technological change, a societal change, or a new scientific knowledge, the risk is new (Jovanović A.S. & Löscher, 2013).

Defining the notion of emerging risks, notion that first appeared in the insurance sector (Ashby & al., 2018, p.4) would lead to a non-exhaustive list of different definitions that you can see in appendix 2, coming from the academic literature (Aven and Flage, 2015, p.67; Mazri, 2017, p.2053). The lack of a uniform and approved definitions of emerging risks is in particular due to the sectors of activity in which the management of emerging risks is carried out.

Nevertheless, this thesis will be based on the definition of Allan et al. who define emerging risks as “*(...) about unclear or changing framework conditions (...). Thus, while we may think of emerging risks as being primarily entirely new risks (...) some are known and familiar risks, but they become new or (re)emerging, as their contextual conditions change*” (Weymann & Egloff, 2018).

The reasons for the choice of this definition are as follows: Firstly, as emerging risks are both threats and opportunities (Aabo et al., 2005, pp.62-66), the definition should not only summarise the impact as having economic losses.

Secondly, the uncertain character of risks and emerging risks (ISO, 2018) should be reflected in the definition. In this case, authors emphasise the unclear and changing nature of the risk. Finally, this definition captures the status of risk that IRGC (2010), Jovanović and Löscher (2013), and Aven & Flage (2015) define as a risk that can be both familiar or new, and emerging/evolving in form.

Regarding the characterisation of emerging risks, that you can see in appendix 3, the notion of characteristics refers, in this work, to what differentiates emerging risks from each other. These characteristics are often found on the axes when mapping emerging risks, which are often associated with the characteristics of high impact events that have a probability of occurrence and consequences that are difficult to predict (Aven and Flage, 2015, p. 62; Florin, 2013, p.319). Whereas features are considered to be the qualifier of an emerging risk.

Indeed, many analyse emerging risks in terms of the likelihood of occurring and the degree of impact if the risk does occur. However, there is no one way to map risks. For example, Chapelle (2020, p. 60) also takes into account the velocity of the risk, i.e. the speed at which the risk evolves and/or the consequences of the risk materialising, which could correspond to the evolution and speed of propagation of the risk.

Regarding now the features concerning emerging risks, the first category of features concerns the type of risk itself. The *CRO Forum* (2006), as well as the *International Actuarial Association* (IAA, 2008) and the *IRGC* (2010) define them as risks that are known, which may be familiar. But which may also be emergent in the sense that they have developed and evolved over time. In contrast to Locklear (2011), for whom these risks are new and have not been experienced in the past.

Regarding the context in which these risks evolve, and according to the *IRGC* (2011), emerging risks arise from new or familiar contexts. In comparison, Allan and al. render their context as arising from a “*complex interactions between strategic objectives, existing risks, risk management interventions, business and regulatory environment, markets and people’s behaviour*” (Allan & al., 2012, p.189), and Aven and Vinnem (2007) add that these risks can take place in a space and time that may or may not be specified.

Locklear (2011) adds that the complexity and interconnectedness that exists between emerging risks is a real challenge for risk management teams. Indeed, the interaction between different existing risks can lead to the emergence of a new risk (Allan & al., 2012, p.189).

Moreover, regarding possible consequences that these emerging risks may have, while Allan and al. (2012) and the *IRGC* (2010) characterise these risks as having unexpected consequences. The latter, as well as the *European Commission* (2016) and the *IAA* (2008), emphasise the highly uncertain degree of these risks and the uncertainty of the consequences that may result from them. The highly uncertain character of emerging risks, as stated by the *CRO Forum’s Emerging Risk Initiative* (2006, p.11), makes it difficult to identify, evaluate and quantify it. We will look at this notion of uncertainty in more detail in the next sub-chapter.

Regarding the ability to identify emerging risks, only Allan and al (2012) and Choo (2005) mention this on their definitions. The first authors pointed out that emerging risks cannot be proven in clear and understandable ways, when Choo (2005) goes further and defines emerging risks as risks that evolve on the basis of erroneous information and therefore cannot be properly identified.

Finally, regarding the procedure for analysing this type of risk, both the *CRO Forum* (2006) and the *IAA* (2008) highlight the difficulty of quantifying it. The latter explaining that traditional risk assessment techniques are not sufficient for assessing emerging risks. Allan et al (2012, p.180) also highlight the difficulty of establishing a causal link between these risks and the losses that may be associated with them, as well as the difficulty of evaluating them in monetary terms due to the lack of information regarding these risks.

Another major difficulty, which we will discuss in the chapter on the people involved, is the difficulty in communicating the emerging risks faced by companies. This can be poor, either because of a lack of valid information or because of cognitive biases, as we will see later on. And finally, the lack of regulation in force is another major feature put forward by the authors and discussed in the chapter on frameworks.

2. Notions linked to emerging risks

a. Black swan types of events

The notion of emerging risks is often confused with the notion of black swans events. These two notions differ in their characteristics, although they are complementary according to Aven and Flage (2015, p.63).

This concept of black swan, developed by Karl Popper, became popular following the publication of Nassim Nicholas Taleb's book: *The black swan: The impact of the highly improbable*. Nevertheless, the beginnings of this notion date back to 1843 and were noted by John Stuart Mill, whose aim was to demonstrate that science cannot prove everything, and that no matter how many white swans we may observe, it does not mean that a black swan cannot exist because it is not visible (Haugen & Vinnem, 2015, p. 1).

Black swan type of events are defined as: *“firstly, it is an outlier, as it lies outside the realm of regular expectations, because nothing in the past can convincingly point to its possibility; secondly, it carries an extreme impact; and thirdly, in spite of its outlier status, human nature makes us concoct explanations for its occurrence after the fact, making it explainable and*

predictable (retrospective predictability)” (Aven & Flage, 2015, p.63; Haugen & Vinnem, 2015, p.1).

According to Allan and al., “*the existence of a black swan is due to our blindness when dealing with uncertainty*” (Allan & al., 2012, p.181). Examples of this type of risk are the terrorist attacks such as the September 11, 2001, the development of the internet, the collapse of a country, or the eruption of the volcano at Fukushima in 2011.

Among the distinctions that exist between this notion and the notion of emerging risks, there is first, the way in which this risk is categorised. Indeed, black swan events are categorised according to the knowledge: unknown-unknowns risks, meaning that these events are totally unknown for scientific community; and unknown-knowns risks, meaning that some scientists are aware of these risks while others are not (Aven & Flage, 2015, p.63).

In comparison with emerging risks, Chapelle (2019) distinguishes three types of categories for emerging risks: risks that are known because they have already occurred and are regularly taken into consideration; risks that are unknown and impossible to predict; and risks that should be known but are often underestimated. However, this type of categorisation is not universal, and some researchers propose another type of categorisation: according to the knowledge of the risk (known, known-unknown, unknown and unknown-unknown risks), or a categorisation according to the source of the risk as developed by IRGC.

Indeed, the latter proposes three categories of emerging risks, of which more information can be found in appendix 4, including “*risks with uncertain impact*”, such as those resulting from new technologies; “*risks with unexpected impact*”, as a result of existing products and services but emerging due to the change in the environment; and “*systemic risks*” resulting from the interaction between different types of risks (IRGC, 2011, p.62).

The main distinctions between these two types of risks, and according to Aven & Flage (2015, p. 63); Locklear (2011, p.11) and *UK government's Office for Science (GOoS)*, are shown in the table below:

Black swan events	Emerging risks
Knowing risks	New or familiar risks that are evolving
Hardly predictable or not	Unpredictable
Extreme impact and consequences	Uncertain impact and consequences

Although there are many distinctions between these two types of risks, they are managed in the same way. Indeed, in both cases, it is necessary to take these risks into account from the earliest warning signals (Aven, 2015, p.86).

Moreover, in both cases, an approach that consists of taking a lessons-learned approach to constantly seek to improve their risk management process is also required. However, for Locklear (2011, p.11) trying to predict such events is a waste of time, as these risks are unpredictable. This is also true for emerging risks given their changing nature in the environment external to companies.

b. Novel risks

Black swan events can be integrated into another category of risks called 'novel risks'. Indeed, according to Kaplan and al. (2020), novel risks are arising from three types of situations: Black swan event; large risk resulting from the interrelation of several small risks which, in isolation, could be manageable; and risk which materialises at such a speed that it is difficult to predict, as in the case of the covid crisis.

Among the main characteristics of this type of risk, which are also found with emerging risks, are the difficulty of quantifying it in terms of probability of occurrence and the degree of impact if it occurs (Kaplan & al., 2020). As well as for emerging risks and black swan type of events, scenario analysis is a regularly used tool for this type of risk.

The difference with emerging risks lies in the way these risks are managed. Indeed, Kaplan et al. (2020) highlight these risks as risks that cannot be managed as current risks and that a CRO would therefore not be inclined to deal with quickly enough. Therefore, the authors advise that it is a Chief Worry Officer who should be able to recognise them and quickly put in place the improvised means to manage them. The role of the CRO in managing emerging risks will be discussed in the following pages

Finally, the lack of literature on novel risks does not allow us to further compare the categories and characteristics of these risks, nor to compare in more details the tools used and the people involved in their management.

c. Uncertain events

Previously, we have seen that uncertainty is one of the main features of emerging risks, and this notion will come up regularly in the rest of this thesis.

Indeed, as said the IAA “*emerging risks are developing or already known risks which are subject to uncertainty and ambiguity and are therefore difficult to quantify using traditional risk assessment techniques*” (IAA, 2008 (as cited in Allan & al., 2012, p.179)).

Nevertheless, this notion of uncertainty is not specifically related to emerging risks but rather to risks in general. As a reminder, ISO (2018) included it as one of the criteria in its definition of risk.

In the context of emerging risks, uncertainty is a feature due to the lack of information to properly identify and assess them (Allan & al, 2012, p.180). This is contrary to Turner and Pidgeon's view (1998 (as cited in Blockley, 2013, p. 32)) that some major disasters can be identified before they occur but that methods have yet to be developed to enable decision-makers to identify the preconditions for disaster with a reliable probability.

The notion of uncertainty, defined by Cantle as “*a lack of certainty. It means that you do not know exactly what is going to happen*” (Cantle, 2013, p.237), is one of the key characteristics of emerging risks and is due to a lack of information that makes the identification and assessment of these risks difficult (Allan & al., 2012, p.179). Indeed, this is also consistent with Blockley's view that says “*(...) all uncertainties are due to limitations in what we know or the conditions for acquiring or understanding*” and adding “*in this sense all uncertainty is knowledge-based*” (Blockley, 2013, p.31).

Previously, we have also seen that the characteristics of emerging risks are the degree of impact, the probability of occurrence, the velocity, etc. In comparison, the characteristics of uncertain events are the fuzziness, the incompleteness and randomness as well as ambiguity, confusion, indeterminacy, and contingency (Blockley, 2013, p.32). Appendix 5 will give you an overview of these characteristics of 'uncertainty'.

There are many similarities between these characteristics and the notion of emerging risks. Indeed, ‘fuzziness’ means “*imprecision or vagueness of definition*” (Blockley, 2013, p.32) and as a reminder, there is no unified definition of emerging risk among scholars.

Concerning the ‘incompleteness’ of uncertain events, it means ‘what we do not know about’. The similarity with emerging risks is the lack of historical data to deal with these risks. Nevertheless, the subject divides the scientific community according to whether emerging risks are known risks, or whether they are new and unknown risks.

Finally, ‘randomness’ “*(...) is interpreted here as the lack of a specific pattern or purpose in some data (...)*” (Blockley, 2013, p.32). This ties in with the difficulty of properly assessing emerging

risks by relying more on certain techniques such as scenario analysis or fault-tree analysis than others (Chapelle, 2019). Nevertheless, like emerging risks, one way to reduce the degree of event uncertainty is through information gathering (Ashby & al., 2018, p.180).

Regarding the assessment phase, the similarity between uncertain and emerging risks is the importance of stress testing to identify these possible risks, as requested by the European Central Bank (*ECB*). Furthermore, banks are also advised to review the investment plan taking into account the profit and loss (p&l) depending on the event (Buehler & al., 2020, p.4). Indeed, a good implementation of governance to manage these risks is not sufficient but must be adapted to changes in the external environment (Dickinson, 2001, p.361).

Finally, according to Jovanović & Löscher (2013) risks characterised as uncertain, as well as risks with a high degree of ambiguity, are likely to become more important in the future, which is similar to emerging risks (Jain & al., 2020, p.2). Whether it is climate risks that will increase in severity, or cyber risks in frequency (*ECB*, 2016; Gramlich & Walker, 2020).

3. Main emerging risks facing the banking sector

Furthermore, climate risks, that the *Basel Committee* is trying to reduce their financial impact and cyber risks, in which the risk of fraud has increased considerably, are among the main risks highlighted in the reports of institutions and organisations.

Indeed, organisations like the *World Economic Forum (WEF)*, the *National Bank of Belgium (NBB)*, *ORX*, *CRO Forum* and the *Emerging Risks Initiative* highlight the main emerging risks, the last two organisations which concerns the insurance sector. Although my research focuses on the analysis of emerging risks in the banking sector, the consideration of these risks also for the insurance sector may be of interest given the number of banks that offer both services such as *Axa Bank*, *Belfius* and *KBC Bank & Insurance* that were interviewed for this thesis.

In these reports for the year 2021, we see that pandemics in general have resurfaced as significant emerging risks due to the covid crisis we went through. In appendix 6, you will find what the *CRO Forum* calls the 'Emerging Risk Radar', where the main trends for the year 2021 and the emerging risks faced by the insurance sector are reported. These risks are analysed according to a time horizon axis, and an impact degree axis. This differs from the *WEF* emerging risk mapping, called the 'Global Risk Horizon' which you will find in appendix 7, and which is represented by the probability of the risk on the x-axis, and the impact of the risks on the y-axis.

Common emerging risks to the report of the *WEF* and the *CRO Forum*, with the highest impact and high probability over a relatively short time horizon or having already occurred, are: first, pandemics/infectious diseases that have increased other risks, such as cyber risks, inflation risks or poverty risks.

Then, extreme weather events such as climate risks which are both physical risks that can indirectly diminish the assets held by banks' clients, or transitory risks which, due to a change in the way investments are made, disrupt the financial market.

Next, there are cyber risks that have increased during the pandemic as bank employees work from home, which can jeopardise computer security. There are also livelihood risks; risks related to the ecological transition and the failure of climate action.

The emerging risks put forward by the *WEF* differ slightly from those put forward by the *ORX*, an association created in 2002 for the management of operational risks for the financial services sector. Indeed, the latter concern the banking and insurance sector whereas those presented by *WEF* are aimed at all sectors in general.

According to the *ORX* report (2020, p.4; 2021)², the top five emerging risks facing the financial services sector in 2021, including banks, are firstly risks related to the emergence of new technologies, followed by cybercrime risks and by climate risks and finally, the fourth are respectively geopolitical and macroeconomic risks, and the last one, people risks. The table below shows the main risks facing the banking sector, for the year 2021.

ORX (2020)	European Central Bank (2021)	National Bank of Belgium (2021)
1. Emerging technologies	IT Risks	
2. Advanced cybercrime	Cybercrime and AML risks	
3. Climate risks	Climate risks	Climate and environmental risks
4. Geopolitics and macroeconomics	Geopolitical risks and tensions between states	Brexit
5. People risks		
		Pandemia

² ORX asked 49 organisations, including 40 banks and 9 insurance companies, to send in a list of their top ten current and emerging risks, identifying a total of 412 current and 281 emerging risks. More information on this survey are available at <https://managingrisktogether.orx.org/sites/default/files/public/downloads/2020/09/orxoperationalriskhorizonsummaryreport2020.pdf>. p.4

a. Major trends that influence emerging risks

In addition, emerging risks are also derived from trends. Indeed, “*emerging risks may include new technologies —for example, artificial intelligence (AI), nanotechnology (...)—as well as economic, societal, environmental, regulatory or political change. While some emerging trends are developing at a slow pace (like demographic changes, societal preferences (...)), others can be fast-changing with disruptive potential (like the development of smartphones over the past decade, alternative currencies right now or AI in the future)*” (Weymann & Egloff, 2018). And authors add that changing trends refer to things “*that may alter the nature, probability and magnitude of expected impacts*” (IRGC, 2015, p.8).

IRGC (2010) goes further by highlighting twelve key factors contributing to emerging risks that you will find in appendix 8. Of which we will find the technological advances, social changes and scientific unknowns that are common to the authors mentioned above and that can also be found within the banking sector.

The appendix 10 categorises the main emerging trends that banks will have to face in 2021 according to the *European Central Bank (ECB, appendix 9)*, as well as you according to the *CRO Forum*, in comparison with a report by *McKinsey&Company* (2021, p.19) and *Deloitte* (2021, p.28).

Among the emerging risks and trends common to these reports are climate change (environmental risks), existing geopolitical tensions between countries, the risks of pandemics and infectious diseases (societal risks), IT and cyber risks resulting notably from digitalisation and new technologies as mentioned by Weymann and Egloff (2018).

The table is divided into different risk categories. However, these are not exhaustive as each organisation has its own categorisation. Indeed, previously we mentioned the difference in the risk axes between the *WEF* and the *CRO Forum*. Another difference between the two reports is the emerging risk categories highlighted in the mapping.

Indeed, the *WEF* highlights six categories: environmental, technological, societal, geopolitical and economical. The last three are only one category in the *CRO Forum* mapping, which adds a category of legal and regulatory risks.

In comparison, Walker and al. (2020, p.1) also have their own categorisations: Ecological, societal and technological. These first two categories are expected to grow in importance in the coming years and an allocation of capital to mitigate these risks must be considered along with their evolution (Gramlich & Walker, 2020, p. 423).

Concerning risk categories more specifically dedicated to the banking sector, and according to the *National Bank of Belgium's* 2020 report, environmental, social and governance (ESG) risks, which include major climate issues, are among the main risks that banks in general and the *Central Bank* are trying to address.

Regarding the risk categories more specifically dedicated to the banking sector, and according to the *National Bank of Belgium's* 2020 report, environmental, social and governance (ESG) risks, which include major climate issues, are among the main risks that banks in general and the *Central Bank* are trying to address.

These ESG risks result in particular from a cultural change in society and new moral demands from consumers for more social responsibility within companies. The *CRO forum* (2021, p.4) also adds that the consideration of these risks results from a greater awareness of the impact of these risks on our society and economy. And that taking these risks into account allows us to ensure sustainable economic and social development and avoid possible reputational consequences if they are not considered.

In response to these new expectations, the *ECB* has issued guidance on "(...) expectations for risk management and disclosure of climate and environmental risks in banks" (NBB, 2021, p.286).

In addition to this, the supervisor has also compiled an inventory of available data needed to measure these ESG risks and is working with the *European Systemic Risk Board (ESRB)* "(...) to develop risk indicators, methodologies, and scenarios to assess the impact of climate risks on financial stability" (NBB, 2021, p.286). In addition, the *European Banking Authority (EBA)* is also working on the integration of these risks into governance and risk management.

Finally, the consideration of these climate and environmental risks has accelerated thanks to the voluntary partnership, created at the end of 2017, between supervisory authorities and Central Banks called *Network for Greening the Financial System (NGFS)*.

This network has put forward the drafting of guidelines on the consideration of these risks by financial institutions and is also a tool to assist in scenario analysis. Future work of this partnership will include the review and collection of data on climate and environmental risks. However, the sole purpose of these publications is to provide recommendations and share information that may be useful to the sector.

4. Framework and regulation on the banking sector related to emerging risks

Nevertheless, many directives and regulations address banks in their risk management but do not provide a tool for managing emerging risks.

Amongst these existing legislations, there is notably the 'Basel Accord', created in 1974 following numerous disturbances in the banking sector (Chapelle, 2020, p.92). These agreements have resulted in three pillars.

The first concerns the regulatory capital that banks must set aside to meet risks, the second concerns an adjustment of the rules of the first pillar, and the third pillar concerns the publication of information on the financial health of the bank and the risks it faces. Since their implementation, these agreements have been the subject of reforms adopted in 2013 following the 2008 financial crisis and a third, adopted in 2017, which will come into force in 2023 after being transposed into national legislations.

Other European directives, notably from the 'Basel Accord's, have also been issued. But again, this one does not address emerging risk management but regulatory capital. Among these, there is the 'Capital Requirements Directive' (CRD), the latest of which, 2019/878, has been transposed in 2019 in the *European Union* with the aim of strengthening the banking union and reducing the risks incurred by banks.

In order to standardise this union, a reporting framework on regulatory capital and prudential regulations addressing both financial and non-financial risks is being put in place, called the 'Common Reporting Framework' (COREP) and implemented by the *European Banking Authority* (EBA) (formerly the *Committee of European Banking Supervisors* (CEB)).

In addition to this, each year an analysis of the banks' risk profile is carried out. This exercise, called the 'Supervisory Review and Evaluation Process' (SREP), consists of ensuring the banks' sustainability, the competence of the management bodies in terms of risk management, the banks' capacity to face losses and finally, the banks' liquidity rate. The purpose of the SREP exercise is to ensure that banks are able to withstand the same financial and macroeconomic shocks.

Previously, we identified climate, pandemic as well as cyber and political risks as the main emerging risks facing the banking sector. We are now going to understand why these risks are major for this sector and why it is important that the regulator puts in place measures to manage them properly.

First, let's see the climate risks, which were the subject of the 'Paris Agreements' that came into force in 2016, aimed at fighting global warming. Which also led to numerous climate marches encouraged by Greta Thunberg, and which brought together hundreds of millions of people.

According to a book entitled: *Green Swan*, written by Bolton and al. (2020), these climate risks are a real challenge for the banking sector because of their uncertainty and rapid evolution, which cannot be anticipated and for which a collective response is necessary. The authors define the notion of a 'green swan' as a "*potentially extremely financially disruptive events that could be behind the next systemic financial crisis*" (Bolton & al., 2020, p. iii).

On April 14, 2021, the *Basel Committee* published two reports on climate-related financial risks³. The first report focuses on the impact of climate risks on traditional risk categories: credit, market, liquidity, operational and reputational risks, via two types of transmissions: physical and transitional. Physical risks, which can materialize at banks with the destruction of data centres in areas suffering from flooding or rising waters. And transitional with the transfer of investments from nuclear powers to more sustainable investments.

The second report focuses on tools for measuring climate risks. It concluded that the traditional process of managing familiar risks does not allow the proper management of climate risks.

On July 8, 2021, *ECB* President Christine Lagarde announced in a press release that climate change will be taken more into account in the *ECB's* monetary policy. She justifies herself by saying that: "*Climate change and the transition to a more sustainable economy affect the outlook for price stability through their impact on macroeconomic indicators such as inflation, output, employment, interest rates, investment and productivity, financial stability and monetary policy transmission*" (Goffin, 2021). The president added that the *ECB* will develop new indicators to monitor the implications of climate change on eurozone financial markets and will also implement stress tests planned for 2022, as well as give greater priority to bond issuers that comply with the 'Paris Agreements'.

Then, on July 14, 2021, an article published by the *BIS (Bank for International Settlements)* underlines the importance of a review of the risk management process, particularly the stress-testing exercise, which is not sufficient to properly manage climate risks in the financial sector. This is due to the fact that these risks materialise over a longer time horizon than for other sectors. This is consistent with the *IRGC's* view that because emerging risks are too uncertain, they cannot be managed in the same way as known risks (IRGC, 2015, p.1).

³ Both reports are available at the following link: <https://www.bis.org/press/p210414.htm>

Regarding cyber risks, they are considered as operational risks, i.e. "*related to losses that could result from inadequate or failed internal processes, improper business practices, systems failures or from external events*" (Aldasoro & al., 2020a, p.4). These risks evolve over time, in both their nature, complexity, severity and frequency, particularly with the development of new technologies (Deloitte, 2018, p.7). They are considered as emergent in the sense that they evolve in the environment and increase with digitization and the ever-increasing number of users and data (ECB, 2016, p.2).

During the Covid crisis, and as confirmed by the *Financial Services and Markets Authority* (FSMA (cited in L'Echo, 2021)), cyber-attacks that have increased sharply in U.S. institutions between February and April 2020, amounting to 13% more than the previous year and 27% of which targeted banks in particular (Osborne, 2020). In total, there were +238% more cyber-attacks that took place in the world during this same period, and nine times more attempts to steal personal data (Talbi, 2020).

In response to these growing threats, the *Basel Committee* published in 2015 an advisory report dedicated to advising financial institutions on the management of these risks, but without legislative value. In addition, the *ECB* established a working group in 2015 called the 'Single Supervisory Mechanism' (SSM) to address cyber and IT risks, open to both euro area banks and banks from non-euro area but EU member states that have requested to join.

Finally, a third emerging risk, identified as having a moderate probability and impact by the *ECB*, is terrorist financing and anti-money laundering (AML) risks. These are regulated by international bodies. This is particularly the case for the 'Financial Action Task Force' (FATF), which was established in 1989 at a G7 Summit and now has 39 member countries and observers such as the *ECB*.

The reports issued by this organisation are mainly the result of non-binding recommendations and guidelines. The *ECB* has put in place, in April 2008, a risk management framework called 'the AML/CFT framework', and transposed into national law in January 2020, it is then up to the Member States to transpose them into their national law.

In addition, there is also a non-legislative action plan proposed by the *European Council* and the *Council of the EU*.

We note that recommendations and regulations are gradually coming into force to better manage emerging risks in the banking sector.

However, this would not be enough. Klinke and Renn (2012, p.280) as well as the *IRGC* (2015, p.1) have asked for better governance⁴ of emerging risks, both collective and integrative, for a while now, based on faster consideration of early-warning signals that can cope also with the uncertain nature of these risks.

Moreover, as said by the S&P Global (2021), “*the current global health crisis has undeniably confirmed that complying with existing risk regulations and standards is not equipping companies well enough with useful tools to cope with external risk events, such as a global pandemic*” (Stauffer, 2021). Especially since most of the regulations in the banking sector concern the establishment of a minimum regulatory capital within banks.

The aim of this thesis is therefore to fill the legislative gap with regard to emerging risks and to provide the necessary tools for their proper management.

5. Stages in the consideration of emerging risks

Regarding the approach used in the management of emerging risks, many organizations, institutions and scholars propose their own corpus of management. Despite the difference in the terms used for each step, as you can see in appendix 11, these steps coincide within the scientific community.

In my work, I based myself on the four steps proposed by Chapelle (2020, p.v): risk identification, assessment, mitigation and monitoring. Among the major differences during these phases between the management of familiar and emerging risks are:

a. Emerging risks identification

During this first phase, the difficulty in managing emerging risks lies in taking them into account from the first early-warning signals (Mazri, 2017, p.2061). Indeed, “*the early identification of emerging risks enables companies to be better prepared for their materialization*” (Stauffer, 2021).

Due to the unpredictable nature of emerging risks, and in order to ensure that the full range of risks that banks can face are taken into consideration, Chapelle (2020, p.22) recommends that companies compare their risks with those from external reports and databases.

⁴ Defined as “[...] *the identification, assessment, management and communication of risks in a broad context. It includes the totality of actors, rules, conventions, processes and mechanisms concerned with how relevant risk information is collected, analysed and communicated, and how and by whom management decisions are taken and implemented [...] and involve scanning the environment and analysing the many signals and trends produced by early-warning systems*”. *IRGC*. (2010). *The Emergence of risks: Contributing factors. Executive summary: IRGC*. Retrieved from: https://irgc.org/wp-content/uploads/2018/09/Exec-Summary_IRGC_ContributingFactorsToRiskEmergence2010.pdf

b. Emerging risks assessment

Once emerging risks have been identified, they are divided into three categories: preventable, strategic and external risks (Kaplan & Mikes, 2012). The first category concerns risks that are influenced by the company's activities, such as those arising from illegal operations, and that can be prevented, for example by the introduction of regulations.

Strategic risks, on the other hand, arise from the activity of the company and are not predictable. Compared to the first category, which are undesirable risks, this category of risks depends on the profile and risk culture within the banks.

Finally, external risks are those which the banks have no influence on. These include natural disasters, changes in macroeconomic trends, etc (Kaplan & Mikes, 2012). A link can be made between this last category and emerging risks, because the impact and consequences of huge catastrophe can rarely be predicted, especially if early warning systems are not taken into account or are ignored, which can lead to large-scale disasters (IRGC, 2015, p.16).

An holistic approach is used in this phase to assess emerging risks because there is an increase in the interrelationship between risks related to technological, macroeconomic, and other changes in our environment due to the digitalisation (ORX, 2020, p.3).

Once emerging risks have been identified and traced back to their causes, an exercise called 'Risk and Control Self-Assessment' (RCSA) is carried out to evaluate the risks according to their degree of impact and probability of occurrence, with a possible distinction for the group and for each activity being made. In addition to this, the author suggests a comparison between the exercise carried out at the beginning of the year and updated after each event that has had an impact on the bank (Chapelle, 2020, pp.62-64).

A third axis, according to the velocity of the event, i.e. the speed at which the event evolves in the environment or the speed at which the consequences are felt within the bank, is also taken into account (Chapelle, 2020, p.60). As for ORX (2021, p.10), it proposes a third axis according to the bank's risk exposure.

Finally, once the RCSA exercise has been completed, the banks then carry out the quantification of the scenarios, that can be either qualitative or quantitative or a combination of both (Ashby & al., 2018, p.194; European Commission, 2017, p.7). Followed by stress testing exercises, imposed by the regulator as we have seen previously. We will not go into more detail here in order to focus more on the organisational aspect of emerging risks and on a more general view of their management, as stress-testing exercises alone could be the subject of a thesis. As well as for the

scenarios quantification which require to manipulate different techniques such as the Delphi method, fault tree analysis, etc.

But finally, mitigation action plans for emerging risks should be reviewed regularly to ensure that they are still effective as risks change (Ashby et al., 2018, p.195; Chapelle, 2019).

6. People involved in the process to analyse emerging risks

a. Chief Risk Officer and the risk management team

This lack of structure has an obvious impact on banks and is a challenge for CROs who serve as a liaison between the supervisory authorities and the bank (Dickinson, 2001, p.365) and works closely with regulatory agencies (Buehler, 2020, p.5).

The CRO role is often given to a senior person who has had an operational role or to someone with an advanced degree and a high level of expertise in areas that require key skills in the implementation of risk management tools and techniques as well as communication tools and a good knowledge of the day-to-day business (Dickinson, 2001, p. 364; Hall & al., 2015, p.10; Holmquist, 2019, p.47; Liebenberg, 2003, p. 42).

This function, which the main role is to “(...) *bring the big-picture thinking*” (Wetekamp, 2021) has grown in importance since the financial crisis of 2008, as shown in the graph in appendix 12.

Among the three main changes in this function since the financial crisis are: An end to the exclusive focus on financial risks and a more holistic approach to financial and non-financial risks; the use of new risk management tools and a forward-looking in addition to a backward-looking; and finally, the shift from a role limited to risk management controls to one of advising the Executive and the BofD on the implementation of a sustainable strategy that respects the bank's risk appetite (Buehler, 2020, p. 3; Gramlich & Walker, 2020, p.428).

Indeed, according to Mikes (2008, p.1), the CRO function also implies a role of 'strategic advisor' in decisions related to the bank's activities. While other academics see the role as a 'strategic controller' who must manage the implementation of good risk management while enabling the bank to remain efficient.

In addition, there are two other roles that Mikes (2008, p.3) identifies with the function of risk managers such as 'compliance champion', which is to ensure that a good infrastructure is put in place, in accordance with the regulations in force. And 'modelling expert', whose role is to model the risks in order to better manage them.

The involvement of the CRO is crucial. A study done by Aebi and al. (2012, p.3220) shows that banks with CROs on the Executive Committee have stronger risk management.

The CRO has a global role in risk management, such as *“to coordinate and lead the internal and external stakeholders involved in the assessment, management and communication of emerging issues”* (IRGC, 2014, p.2). However, it is not intended to dictate to the other lines of defence but to facilitate discussions and collect the data necessary for the proper management of emerging risks and to ensure the proper participation of everyone involved in risk management (IRGC, 2014, p.1).

However, the CRO does not act alone. Indeed, the function is included in the second line of defence (Holmquist, 2019, p. 49), has a risk management team whose main role is to advise the BofD on risk appetite, ensuring that limits are not exceeded, through the implementation of key risk indicators (KRIs) and finally, giving recommendations on risk-taking according to the bank's objectives and strategy and implementing the necessary controls to mitigate these risks (Chapelle, 2020, p.118).

Holmquist completes with a more global view by pointing out the first responsibility as *“be the architect of the bank's enterprise risk management (ERM) program and framework”* and the second one is to *“provide effective challenge to the first line of defence with regard to risk taking”* (Holmquist, 2009, p.46).

Furthermore, among the three main changes in the CRO function following the 2008 crisis, we cited a forward-looking approach in addition to a backward-looking approach. This approach takes place during the risk identification and assessment phase. Holmquist (2019, p. 50) and Mikes (2009, p. 30) also add the importance for the risk management team to take into account past events and see what it can learn from them. As well as adapting actions taken to mitigate risks, while looking to the future (Holmquist, 2019, p.50; Mikes, 2009, p.30) and remaining alert to any new or existing risks that may evolve and have a different impact and consequence than before.

Moreover, the second line of defence is responsible for sharing information with both the BofD and the Executive Committee, consisting of the CEO and CFO (Holmquist, 2019, p. 46; Liebenberg, 2003, p.42; Mikes, 2008, p.13).

This reporting to the top management is important (Chapelle, 2020, p.4). Indeed, a study by Mikes & Kaplan (2012) in the aftermath of the 2008 crisis showed that, during the crisis, banks that had more exchange with their BofD and Executive Committee would have survived better than those where little exchange was established.

The authors also add that banks that survived the crisis, such as *Goldman Sachs* and *JPMorgan Chase*, had a strong internal risk management function with good leadership where the CEO is also involved in risk management and add the importance of adopting a holistic approach where all categories of risk are considered.

Furthermore, another study by Aebi et al (2011, p.3224) shows that banks where information is reported directly to the BofD would have performed better than those reporting exclusively to the Executive Committee, as the latter does not have the same interests as the CRO, which could lead to a neglect of risk consideration.

Nevertheless, when reporting information, it is important not to use overly technical terms in meetings with the board to ensure that key risks can be understood by non-risk professionals, for example by adding an explanatory note or using colour coding according to the severity of the risk (Hall & al., 2015, p.11).

Many scholars (Chapelle, 2020, p. 155; IRGC, 2014; S&P Global, 2021) advocate the implementation of awards, as part of the company culture, for those involved in risk management. And in some cases, disciplinary sanctions for non-reporting of risks, which may consist of a penalty in the performance bonus, the latter being a KPI in the employee performance evaluation, such as lack of respect for risk appetite, lack of action plans and controls in place, lack of frequency of meetings where risks are identified and analysed, lack of data or non-compliance with compliance rules imposed by the legislator, etc.

According to Buehler and al. (2020, p.3), the implementation of a good risk culture and communication strategy within the bank is the role of the CRO, as well as the importance of adequate governance.

b. Board of Directors

The implication of the BofD in the risk management is important. Therefore, he or she must have an understanding of the main risks that the bank may face and what is being done to manage these risks (Aabo & al., 2005, p.62).

Its role consists of deciding on the bank's risk appetite, assessing risk exposure, overseeing the risk management program and ensuring that risk management is aligned with the bank's strategy and objectives, validating the scenarios produced by the risk management team and that the controls in place are sufficient (Holmquist, 2019, p.51; Chapelle, 2020, p.175).

c. Executive Committee

According to a survey of 57 financial institutions conducted by *Deloitte* (2021)⁵, in 73% of cases, emerging risks are reported periodically to the BofD along with other risk reports. However, the involvement of the Executive Committee is also important. The study also shows that only 65% of Executive Committee and/or the Risk Management Committee monitor emerging risks.

The Executive Committee is mainly involved for the risk mitigation phase where its role is to decide to outsource the risk or to decide on the amount of money needed to be allocated to risk mitigation for the purchase of insurance for example (Dickinson, 2001, pp.364-365).

Another responsibility of the CEO that concerns both him/her and the CRO is to ensure that risk managers challenge opinions in the risk identification process and avoid them guiding positions with the information they know and directing the opinion of teams, which can lead to organizational biases as we will see in the section on cognitive biases (Kaplan and Mikes, 2012).

d. First line of defence

In addition to take place at the top-down level, information sharing also needs to take place at the bottom-up level, i.e. with the different business sectors. Shared information includes “(...) *what risk there is (identification), what might happen (assessment), and what might be done about it (response)*” (Christiansen & Thrane, 2014, p.428).

Previously, we spoke about the importance of communication and transparency within the company, which several researchers have highlighted as part of the company's culture. This would allow the bank's employees to be aware of the main risks facing their company and the knowledge and skills required to deal with them (Fraser & Henry, 2007). This top-down approach should ideally be carried out four times a year (Chapelle, 2020, p4).

The first line, considered as the risk owners (Holmquist, 2019, p.48; Chapelle, 2020, p.116), are responsible for decisions made in the face of risk, and for their consequences as well as for managing them without exceeding the tolerance threshold.

Chapelle (2020, p.117) also adds that they are responsible for the risk assessment and mitigation phases. In addition, their roles also include the collection of incidents, the evaluation of risks and associated controls, the definition of actions based on the risks identified and allowing the threshold of appetite to be respected.

⁵ Deloitte conducted a survey of 57 financial institutions worldwide, 16% of which have banking as their core business. More information on this survey is available at https://www2.deloitte.com/global/en/insights/industry/financial-services/global-risk-management-survey-financial-services.html?id=gx:2em:3int:GRMS_12:5eng:6fsi:20210102

We refer to their involvement mainly during the risk identification phase, as also demonstrated by Fraser and Henry (2007) and Kaplan and Mikes (2012).

These risk identification meetings are held annually or semi-annually and bring together the managers responsible for the different types of risks as well as the management committees and business line managers, and often take the form of a workshop (Chapelle, 2020, p.4).

e. Internal audit and audit committee

Finally, the third line of defence includes internal audit, an independent function in the process of (emerging) risk management, unlike the first two lines of defence, but one that is essential (Chapelle, 2020, p.120; IAA, 2004). One of its objectives is to ensure compliance with the regulations in force.

Indeed, Buehler & al (2020, p.3) add that the risk management process should be more professional and require more independence from the audit department whose role is in particular maintaining a relationship with the BofD on risk management and by providing required controls.

Nevertheless, opinions differ with regard to the role of this internal audit department in the (emerging) risk management process. According to the *Institute of Internal Auditors* (IIA, 2004), their role includes assessing the risk management and reporting process, advising management on how to deal with risks and providing assurance to the board that risks are being properly managed, acting as a consultant by proposing tools and techniques suitable for risk management and the implementation of controls. But it cannot establish the bank's risk appetite, which is the role of the BofD on the advice of the CRO, nor can it identify and assess risks or impose a risk management process (Fraser & Henry, 2007, p. 397).

The *IIA* concludes by saying that the responsibilities of the internal audit function should be defined in the audit charter and approved by the board (2004).

According to Turnbull and Zaman (2001 (cited in Fraser & Henry, 2007, p.398)), they see their role as a reviewer and their lack of involvement in the day-to-day operations of the bank, as well as their lack of risk management expertise, may be a hindrance to their involvement in risk management.

f. Other teams involved

In addition, to the 'Senior Risk Officers', who indicate operational, reputational and other types of non-quantifiable risks to the top management agenda, Mikes (2009, p.34) goes further and, based

on a study carried out at two major banks⁶, she highlights two more profiles of specialists involved in risk management. Such as ‘silo risk specialists’, who measure and assess risks individually and ensure that each risk does not exceed the threshold. And ‘risk capital calculation specialists’, who assess the bank's risk profile and set limits to ensure that these thresholds are not exceeded and calculate the necessary capital to be allocated to the risks.

You will note that in this section dedicated to the people involved, there were no distinctions made between emerging risks and other risks, as the CRO and other functions does not stop at considering emerging risks alone but takes into account both financial and non-financial familiar and emerging risks.

g. External consultants

Finally, a last function involved on the managing of (emerging) risks are the external consultant. According to Kaplan and Mikes (2012), expert advice is important when identifying the bank's risk profile and setting up controls. Especially because investment banks have their risk profile strongly impacted by market changes and volatility.

Therefore, external consultants are useful to challenge and support risk managers to ensure that risks are continuously controlled and remain acceptable in comparison to the bank's risk profile.

External consultants could also have a role to play in holding meetings where risks are discussed to avoid any kind of cognitive bias and to challenge the employees' positions in the risk assessment (Chappelle, 2020, p.17).

h. Cognitive biases

Indeed, according to IRGC (2014), when assessing risk, the social construct and perception of it can lead to an assessment that does not correspond scientifically.

According to some scholars, risks are considered as “(...) *not real phenomena but mental constructions resulting from how people perceive uncertain phenomena and how their interpretations and responses are determined by social, political, economic, and cultural contexts and judgments*” (Klinke & Renn, 2012, p.279).

This notion of cognitive biases appears mainly in the scenario analysis where risks are assessed in the workshops. Appendix 13 will give you a non-exhaustive list of cognitive biases and deficiencies faced by actors in the management of emerging risks, and a more exhaustive list can

⁶ More information regarding this study is available at: Mikes A. (2009). Risk management and calculative cultures. *Management Accounting Research*. 20(1). 18-40. Doi: <https://doi.org/10.1016/j.mar.2008.10.005>

be found in articles written by Iraci and Rogers (2018), Locklear (2011, p.7-8) and Taleb (2007, p.8 (cited in Locklear, 2011, p.14)).

In addition, cognitive biases “(...) *refers to the reliance on limited information or preconceived notions when making decisions*” (Iraci & Rogers, 2018). And as Locklear (2011, pp.7-12) states, cognitive biases explain why emerging risks are not taken into consideration at the earliest warning signals and can become devastating for banks. Therefore, decision making in the case of emerging risks can be irrational due to the lack of information to do so, as decisions are made on the basis of judgements.

Indeed, Renn, Klinke & Van Asselt (2011) add that humans tend to make judgements based on past events, but we have seen that when dealing with emerging risks, the lack of knowledge about these risks and their uncertainty makes them difficult to identify and assess.

In order to avoid these cognitive biases, Chappelle (2020, p.17) recommends that the experts involved in the risk assessment should not have access to empirical evidence and observable data in advance, as these may influence the discussions. She also suggests the presence of external experts and finally, that the exercise should first be carried out individually in writing before being discussed collectively.

In addition, Iraci and Rogers (2018) propose the following solutions: Being aware of the biases that can induce our choices, this awareness allows us to reduce them (bias awareness). Another way is to take the time to analyse each piece of information from different sources and to accept them as they are given to us and not as we would like to see them (situational awareness and different information sources).

Finally, it is also important that several opinions are taken into account, and that the opinions challenge each other, in order to ensure that their decision making can be as realistic and appropriate as possible to the risks faced by the company (constructive conflict and devil's advocate).

Part 2: Empirical research

Chapter 1: Methodology

1. Subject of study and problematic

In the first part of this thesis, we have seen that the concept of ERM is widely used by banks but is not sufficient to identify emerging risks. We have also seen that regulators and supervisor do not have sufficient insight and knowledge of these risks to provide sufficient recommendations and guidelines for banks to deal with them. Nevertheless, these require banks to prove that they are able to deal with these risks with sufficient action plans.

However, the consideration of these risks is crucial for banks as they can be a risk, as well as an opportunity, for banks as the IRGC (2014) states “*emerging risks and opportunities are often interrelated, and it is as important for organisations to create conditions for opportunity management*” (IRGC, 2014, p.1).

2. Research question and objectives

The objective of this research is to highlight recommendations enabling banks to deal with emerging risks. Therefore, my research question is the following:

‘How do companies, in the banking sector, build a process to consider emerging risks.’

To do this, a comparison between the literature review and interviews conducted with banks will be carried out, where the following questions will be addressed.

1. How banks define the notion of emerging risks?
2. What are the main emerging risks and trends facing banks?
3. What are the reasons that emerging risks are taken into consideration by banks?
4. Who are the people involved in managing emerging risks?
5. At what stage in the management of emerging risks do banks use external consultants?
6. How do banks collect information needed to manage emerging risks?
7. How do banks process to consider emerging risks?
8. How is information on emerging risks shared within banks?
9. How often are emerging risks reported within the banks?

Finally, these questions will be answered in a third part, dedicated to the corpus of good practices, according to the four steps identified by Chapelle in risk management (2020, p.v): identification - assessment - mitigation - monitoring.

3. Research methodology

a. Methodology used for the interviews

▪ Data collection

In the context of this research paper, I had the opportunity to interview eight banks, the name of which and the function of the interviewee can be found in the table below:

Name of the bank	Function of the interviewee	Type of bank	Size of the bank in Belgium	Activities of the bank	More Information regarding the assurance activity
Argenta	Chief Risk Officer	Commercial bank	[500;1,000] employees		
AXA Bank	Chief Risk Officer	Commercial bank	[500;1,000] employees	Banking and insurance	The Bank is one of the supervisory authorities for the insurance activity
Belfius Bank	Chief Risk Officer	Commercial bank	[5,000;10,000] employees	Banking and insurance	The insurance activity is subject to bank supervision.
Bpost Bank	Chief Risk Officer	Commercial bank	[0;500] employees		
Euroclear Bank	Chief Risk Officer	Securities clearing bank	[1,000;5,000] employees		
KBC Bank & Insurance		Commercial bank	[10,000;20,000] employees	Banking and insurance	The Bank is the supervisory authority of the group.
World Bank	Chief Operational Risks Officer	Financial Regulator bank			
/	/	Investment bank	[1,000;3,000] employees	/	

The interviews, which took place from early May to mid-June 2021, were all conducted remotely, via Teams or their own meeting network, in English and for an average duration of sixty minutes.

Most of the interviewees were CROs, but for two banks it was one of the people from the Risk and Compliance department as the CRO was not available. All of them received the interview grid when they were contacted so that they could familiarise themselves with the questions and collect the information, needed to answer them, in advance.

The qualitative interviews were conducted in a semi-structured manner in order to allow the interviewee to speak spontaneously and to gather as much information as possible while going more in-depth on certain themes and allowing me to highlight information that I found important and that could contradict or distinguish from other interviews. As a result, the questions were not asked in the same order as defined in the grid and some questions could not be asked either because the interviewee answered them spontaneously or because of lack of time.

After each interview, I asked if their names, functions and/or company names could appear in my thesis. Some commercial banks have requested that the name of the bank not be linked to the information given. And you will also find that one bank has requested total anonymity, so we will limit ourselves to saying that it is an investment bank with between 1,000 and 3,000 employees.

▪ Data analysis

When transcribing the interviews, which were carried out in their entirety, I did a categorical content analysis, i.e. I divided the interviews into ten categories: 'definition of emerging risks', 'the main emerging risks that the bank (has) faced during the last year', 'the sources used to collect information on these risks', 'the people involved in managing emerging risks', 'the number of times per year that risks are analysed and reported', 'how information on these risks is shared within the bank', 'the different steps and tools for analysing emerging risks and the timing for each step', 'the use of external consultants to manage these risks', 'how these emerging risks relate to other risk categories', 'how these emerging risks relate to the bank's objectives and strategy'.

To protect the confidentiality asked by commercial banks not to create any links between information they shared and their name, a random letter between A and D will be given to each of them throughout this second part in order to allow the reader to identify the links between the information given without being able to say which banks the information comes from.

Regarding the Bank C it is important to precise that the CRO interviewed is working for the group risk department and is responsible to gather information from all the countries where the bank is.

Meaning that, unlike the other commercial banks interviewed that share information from the country point of view, the CRO of the Bank C shares information from a group point of view.

Furthermore, of the banks interviewed, *Argenta* and *KBC Bank & Insurance* have insurance activities in addition to their banking activities. Although they told me that their main emerging risks differ according to their activities, the risks are managed in a common way, with the same method and the information is reported in the same way, as we will see later.

Also, regarding *Euroclear Bank*, the CRO is the one for the Bank but not for the Group, Bank which is one entity of the *Euroclear SA/NV* Group and which represent more than 70% of the group' profit, and balance sheet, according to the interviewee.

Chapter 2: Analysis of the emerging risk management process in the banking sector

Before moving on to the interpretation of the data, we will define the types of banks interviewed.

We identify four types of banks, commercial banks, investment banks, clearing banks, and financial regulators and institutional banks.

First, regarding the commercial banks, it is defined as “*a financial institution that accepts deposits, offers transfer and savings account services, and makes loans*” (Kagan, 2021) such as *Argenta*, *AXA Bank*, *Belfius*, *Bpost Bank* and *KBC Bank & Insurance*.

Secondly, investment banks are defined as “*a financial institution that helps individual or organisations to raise capital and provide financial consultancy services to them*” (Hargrave, 2020). As this thesis does not only focus on Belgian banks, and taking into account the abolition of the Glass-Steagall Act in 1999, it would be interesting to know if the historical distinction between the commercial and investment banks was also reflected in the risk approach of these two types of financial institutions and if there are repercussions on their risk management today.

Indeed, in 1933, an American law, the ‘Glass-Steagall Act’, forced to separate commercial banking from investment banking to protect the deposits of their customers. After the Great Depression of 1929, more than 5,000 US banks went bankrupt. The President Clinton cancelled the law in 1999 to install more freedom on the financial market (Heakal, 2020).

Finally, *Euroclear Bank* is one of the so-called clearing banks and *World Bank* is part of the ‘Financial regulators and institutional banks’.

Taking into account the different banks that exist, we will now analyse the information and compare what the banks have to say in order to draw up a corpus of good practice. This analysis will be done along several dimensions. A comparison will be made between commercial banks, investment bank, financial regulator bank and securities clearing bank.

Within commercial banks, two sub-comparisons will be made, one between large banks versus small banks. Then, another comparison will be made between banks that have a purely banking activity versus those that have both a banking and insurance activities.

The reason for these comparisons is that, for example, the arrival of new regulations impact on the banks' activity and their business model to ensure that the possible shock of emerging events does not lead to too great economic loss, jeopardising the bank's liquidity and solvency and its reputation. However, these banks are not all subject to the same regulations, or even zero regulation for *World Bank*. This organisation's mission is in particular to finance projects in developing countries with the aim of notably fighting poverty, which is why a comparison is necessary.

Another reason why such a comparison will be made is that in smaller commercial banks, there are not as many people involved in risk analysis compared to larger banks, which could influence the roles assigned to people in the management of emerging risks and the reporting of information.

Finally, for banks with both a banking and an insurance business or for holding banks, the way in which information is shared within the bank is not the same. Either because they do not face the same degree of importance of emerging risks depending on the activity or because the holding bank has several countries where information has to be collected and shared or because their maturity regarding the management of (emerging) risks are not the same, as we will see.

1. How banks define the notion of emerging risks?

The definitions of emerging risks given by the banks interviewed, that you can find on the table below, will be broken down and analysed according to four key questions that I have established: 'are the emerging risks totally unknown?', 'in what context does these risks evolve?', 'what are the consequences derived from these risks?' and 'are these risks difficult to quantify?'.

	Definition of emerging risks
Type of banks	
Large commercial banks	Bank A: Emerging risk is a risk that we know and that is not yet materialize but we see coming and that will materialise in an important way and which will affect the risk profile of the bank. Bank B: Emerging risk is a risk that we know or that we should know but still evolving and not yet clear identified as a risk. But still unknow whether it is a risk or not, its scale and the possible impact it can have, and for which the risk management is not enough mature to deal with. Bank C: Emerging risk is a specification or something that already exists or maybe something that intensifies. It is a little bit newer risk which is not going to materialize tomorrow but which is becoming increasing and for which there is no impact or little one on the short time and potentially big impact on the long term. Bank D: Emerging risks is a hotspot risk that is important or becoming important for which the materiality of the bank is not enough mature to properly manage it.
Small commercial bank	Emerging risk is a risk that is not yet occur but for which there are some signs that something is happening and that is emerging from change in the external environment that affects or may affect the activities of the bank.
Investment bank	Emerging risk is a risk which is not yet closely monitored by the bank but that can have on influence on the future of the bank.
Euroclear Bank	Emerging risks is something uncertain to look forward and can be either known risk, known-unknown risk or unknown-unknown risk.
World Bank	Emerging risk is a risk usually known that is growing in importance and that suddenly everybody pays attention to it.

Firstly, regarding the definition of emerging risks and the risk in itself, according to commercial banks, three told me that these are risks that we know in general. Although for Bank B it is not

possible to recognise in advance whether the event can be considered as a risk or not, and which exists but may intensify depending on the environment.

The Bank C considered it delicate to qualify these risks as emerging risks because if we talk about climate risks and cyber risks, these are risks that have been analysed for many years and cyber risks are risks that materialise on a daily basis. As a result, it is difficult to call them emerging risks. This is in line with the *World Bank's* view that these risks are usually known. In comparison, *Euroclear Bank* defines emerging risks as risks that may cover both known risks, known-unknown risks, and unknown-unknown risks.

Turning now to the context within which these risks evolve. The small commercial bank and Bank A and B describe them as risks that can already be seen, arising from changes in the external environment, although these have not yet materialised.

Nevertheless, two of the large commercial banks, as well as the small commercial bank and the investment bank, indicate that these risks may impact on the future of the bank and its activities, although their impacts are not yet clear, such as the case for climate risks which the biggest impact is still to come, as said the Bank C.

Moreover, regarding their possible impacts, Bank D calls these emerging risks, 'hotspots risks', due to their possible impact, and the focus on their management requested by the BofD, as well as a more detailed analysis of these risks in particular. In comparison, the large commercial bank C says that the impact may be nil or small in the short term but huge in the longer term, while for bank B the impact is not predictable. Finally, only *Euroclear Bank* mentions that emerging risks could lead to a threat as well as an opportunity and that this is explained by the uncertainty of this type of risk.

Concerning the way these risks are managed, Banks B and D indicate that their structure is not mature enough to take them into account. The challenge for banks is to ensure that their risk management systems remain sufficiently robust to deal with risks, that are increasing in frequency and severity. Moreover, according to a report published in 2021 by *McKinsey* on risk, banks have one of the most mature risk management systems compare to other sectors.

The investment bank adds that these risks are not yet closely monitored and *Euroclear Bank* stresses the importance of looking to the future to better identify it, while for *World Bank*, these are risks that everyone pays attention to suddenly.

In conclusion, and according to the common ideas to banks interviewed, we cannot clearly see a distinction between the definitions of the different type of banks. In general, we could summarise

by saying that emerging risks, also called 'hotspots risks', are potential risks, often known and evolving according to the external environment, with a time horizon of more than five years. And which have important consequences on the activity of the banks on the long term, even though they are not easily identifiable in advance, but which have not yet materialised and for which the traditional risk management structure is not sufficient to manage them.

The reason why elements of this definition are attributable to emerging risks, and not to familiar risks, as shown in appendix 1, are the fact that these risks are not easily identifiable, that they have not yet materialised, and that the traditional risk management structure is not sufficient to manage these risks.

And the similarities between the definition of emerging risks, given by Weymann and Egloff (2018) and the one that I wrote on the basis of the interviews, result from that these risks can be new, or familiar, but in this case, emerging in the sense that they evolve following changes in the environment.

2. What are the main emerging risks and trends facing banks?

Now that we have considered how the actors describe emerging risks, let us consider the main emerging risks faced by the banks interviewed. A table showing the main emerging risks identified by the banks and the categories of risks affected is provided in appendix 14.

The different emerging risks faced by banks have been divided into two categories, which in turn are divided into six sub-categories. Sector risks will be considered as external risks that the bank's strategy does not directly influence and control. In addition, two new risk categories will appear within the so-called internal risks: outsourcing risks and business risks.

The first category of risks concerns external risks, i.e. risks evolving in the external environment, not being risks directly linked to the bank's activity or to internal decisions. This category of risks includes environmental risks, such as climate change risks; societal risks, such as the covid pandemic; technological risks, which include cyber risks such as fraud or IT risks due to digitalisation and new technologies; geopolitical risks such as the Brexit; economic risks, such as periods of inflation and rising interest rates decided by central banks; and finally legal, compliance and regulatory risks. The second category of risk concerns the bank's internal risks, i.e. risks influenced by the strategy and choices made by the management, including outsourcing and strategic risks that include business risks.

The first reason of this categorisation is that banks told me that they do not assess emerging risks separately and add that these risks are included in the traditional risk taxonomy. In addition, banks

stated that they did not have teams responsible for emerging risks and that these were managed by the various teams such as IT risks team, credit risks team, compliance risks team, etc.

Another reason for such a classification is that for all banks interviewed, the bank's objectives and strategy are adapted to the risks they may face. As these risks do not have the same impact on the bank's business models, either according to their degree of materialisation (cyber-attacks that happen on a daily basis vs. events that result from climate change that is not yet fully materialised); or their duration over time; or their uncertainty (new regulations vs. climate change), it is important to make a distinction between them.

And finally, the third reason for this categorisation lies in the process to mitigate these risks. Indeed, external risks tend to impose themselves on banks. And in addition to adapt their objectives and strategy to the risk, they must put in place the necessary preventive controls to mitigate them while regularly scanning the environment in which they operate. Whereas in the case of risks related to internal decisions such as outsourcing to third parties, it is necessary to make the right choices internally and to find the right clients with whom possible risks and controls are discussed in advance

Let us start by analysing the main emerging risks related to the external environment. Four of the five commercial banks interviewed highlight climate risks as one of the main risks, risks also indicated as major for *Euroclear Bank* and part of the ESG risks highlighted by the investment bank. It was surprising to hear Bank D identify these risks as financial risks. Also, three other commercial banks noted the financial impact of these climate risks, as also shown in the report published by the *Basel Committee* on 14 April 2021 entitled 'Climate-related financial risks'.

These climate, and ESG risks in general, are increasingly taken into account by banks, as indicated by Bank A, which requires that the '17 United Nations Sustainable Development' goals as well as the CO2 reductions, are indicated and respected by the other party when the bank makes contract with third-party.

Such consideration of climate risks by banks is not surprising. Indeed, according to the ORX report (2020, p.6), two-thirds of the 49 banking and insurance companies that participated in their survey, listed a risk related to climate change in their top ten current and emerging risks⁷. And

⁷ ORX asked 49 organisations, including 40 banks and 9 insurance companies, to send in a list of their top ten current and emerging risks, identifying a total of 412 current and 281 emerging risks. More information on this survey are available at <https://managingrisktogether.orx.org/sites/default/files/public/downloads/2020/09/orxoperationalriskhorizonsummaryreport2020.pdf>

38% of respondents to a *Deloitte* report (2021, p13)⁸, on a survey of 57 financial institutions say that ESG risks are the most important risks in the coming years for these financial institutions and adds that 40% of respondents say that ESG risks are included in risk reports to the BofD.

Nevertheless, still according to Bank A, the regulator will only take into account environmental risks, without really caring about societal risks and fears that people with low incomes will no longer be able to invest in quality housing, especially because of the introduction of ‘energy performance certificates’. This can be a brake on the inclusive and societal model that banks are trying to adopt in order to act as a model in society.

Besides, climate risks are taken into account in the so-called ESG risks. In one of the other two categories, the societal risk category, it was surprising to find that only the small commercial bank mentioned pandemic or infectious disease risks as a major risk. The investment bank added that covid: “*was a surprise for everyone. But the category exists, it is just the extend of the crisis that was not anticipated*”, nor the impact on the continuity of its business. And added that ESG risks are part of the major emerging risks it faces and that it has not yet totally taken into consideration unlike to cyber risks. In addition, unlike other sectors, the banking sector, as well as the retail and information sector, were not affected too much by the covid crisis due to the digitalization of products and services and thanks to state aid to face the possible liquidity and credit risks that the crisis could have caused.

In the case of *World Bank*, it has highlighted aircraft crashes as one of the potential risks it needs to be prepared for. Indeed, following the crash of the Ethiopian Airline Boeing 737 Max, flying from Addis Ababa to Nairobi to assist a conference, the organisation has lost one member, compared to approximately twenty people died who were affiliated with the *United Nations*.

Since this accident, the organisation realised the importance of not having all of its employees in the same plan to avoid human losses and avoid losing senior managers that are involved in the organisation, which could have disastrous consequences on its activity.

Turning now to technological risks, highlighted by all commercial banks interviewed as well as by *Euroclear Bank* and *World Bank*. These risks include cyber-attacks, such as fraud risks that can lead to phishing and data leakage and jeopardise private data. As well as risks related to new technologies such as artificial intelligence, and digitalisation. These are becoming more and more

⁸ *Deloitte* conducted a survey of 57 financial institutions worldwide, 16% of which have banking as their core business. More information on this survey is available at https://www2.deloitte.com/global/en/insights/industry/financial-services/global-risk-management-survey-financial-services.html?id=gx:2em:3int:GRMS_12:5eng:6fsi:20210102

important for banks and take place on a daily basis but their nature as their severity and impact on the banking sector (or all sectors in general) are intensifying.

Indeed, an analysis by the *International Monetary Fund (IMF)* in 2018, shows that a large-scale cyber-attack impacting 50 countries could collapse the financial markets and results in losses equivalent to US\$270 billion to US\$350 billion (*Deloitte*, 2021, p.32).

In addition, the rating agency *Fitch* has taken the decision to incorporate the cyber security of financial institutions into its rating. According to the *AXA Group's* Director of Research - Security (2019), the reason why these cyber risks are still described as emerging risks, even though they occur on a daily basis, is that there is still little knowledge of these risks and the historical data does not allow for the necessary structure to be put in place to manage them properly.

In addition, regarding geopolitical risks, it was surprising that none banks mentioned Brexit during the interviews, that may have had an impact on market risks. One of the reasons could be that the risks having materialized, the uncertainty about the Brexit would no longer exist. And that the supervisor's agreements on this Brexit are now known and taken into account in the analysis of this risk. Nevertheless, two commercial banks as well as *Euroclear Bank* talked about these geopolitical risks as having an influence on the external environment of the banks but that they are not really an issue in Belgium.

Furthermore, none of the banks mentioned the impact of the US embargo, initiated by Donald Trump during his presidency, despite that it has consequences for banks financing projects in China and Iran.

Regarding now the economic risks, they have been highlighted by four commercial banks as well as by *Euroclear Bank*. One reason why banks put forward this risk is the fear of a period of inflation following the covid crisis with an impact on interest rate risks.

And finally, for the last category of risks in the external environment raised by all large commercial banks, as well as by the investment bank and *Euroclear Bank* is legal-compliance- and regulatory risks such as anti-money laundering (AML) risks.

These risks, which concerns more the banking activity than the insurance one, relate to the regulator's new and increasing legal and supervisory requirements for banks. A concrete example is the application of the GDPR rules on personal data protection in financial institutions of the European Union, which came into force in May 2016, giving consumers more freedom in the use of their personal data. One of the commercial banks told me that in their view, regulatory risks are not a risk as such but of the context in which banks operate.

Now, regarding internal risks, risks as a result of the bank's business and strategy, and more particularly outsourcing risks, these have only been formulated by one large commercial bank which has both a banking and an insurance activity and which outsources some of their services to partners with greater expertise in the field, such as for IT risks.

Concerning strategic and business risks, these were formulated by two commercial banks as well as by the investment bank and *Euroclear Bank*. One of the reasons why these risks are considered emerging is the arrival of new competitors in the banking sector. In addition, and as indicated by the small commercial bank in the interview, the business model of banks needs to be reviewed to ensure that customers retain confidence in their banks.

Indeed, although banks are in a highly regulated sector, they must still remain competitive in a market where consumer preferences are changing, and where sustainability and the transition economy are increasingly valued. Indeed, new cooperative, sustainable and transparent banks, such as *New B Bank*⁹ or with the arrival of wooden bank cards, launched in 2021 by a London-based start-up, part of the profits from which will be reinvested in tree planting, are entering the market. In appendix 15, you will find more information on why ESG risks are increasingly taken into account by banks and how they are responding to changing consumer preferences.

To conclude, while geopolitical, climate and cyber risks are the three main risks raised by both the *ORX* database, the *CRO Forum*, the *WEF* and the *Central Bank of Belgium*, it is mainly the latter two that are mostly highlighted by all banks interviewed. In addition, legal-compliance- and regulatory risks are also one of the main emerging risks for all large commercial banks and the investment bank as well as by *Euroclear Bank*.

3. What are the reasons that emerging risks are taken into account by banks?

Let us now try to understand why these main emerging risks mentioned above represent risks for banks.

We have seen in the first part that there is a lot of legislation on risk management in general, although mainly on financial risks, and that the regulator requires a minimum capital to cover all these risks. But except some recommendations, there is no regulation concerning the management of climate risks or cyber risks more specifically. Nevertheless, taking these risks into account and managing them properly is essential.

Indeed, one of the large commercial banks interviewed, with both banking and insurance activities, justifies the importance of taking these emerging risks into account to ensure financial

⁹ *News B* is a bank that also has an insurance service and invests in funds that aim to be more sustainable

stability and compliance with regulations. In addition, it also adds to keep the trust of their customers and that these customers can be sure that both their money and their data are protected and provide them with the necessary information in case of cyber risks.

For another commercial bank with both banking and insurance activities, the reason for taking emerging risks into account seems to lie more in the fact of avoiding economic impacts that could have been avoided with the implementation of a good risk management system. Indeed, this bank said that emerging risks were risks that have not yet been identified and whose impact was unclear, particularly because of the evolving nature of the risk. As a result, emerging risks such as climate risks and cyber risks are regularly assessed due to their still uncertain nature and for which the bank wants to mitigate economic losses as best as possible.

This view is quite similar to the one of the investment bank, for which the consideration of emerging risks, which it considers difficult to monitor closely, is important to ensure that all risks are well managed. Another reason also pointed out is to meet the expectations of the board, and that not managing these risks would be a failure as this would mean that he would not respect his mandate as a CRO.

Moreover, only *Euroclear Bank* emphasised the possibility of new opportunities when considering emerging risks, while the other banks emphasised the risk of threats. Such as *World Bank*, which sees emerging risks as a potential obstacle to achieving organizational results and performance.

In addition to the importance of considering emerging risks, for reasons of financial stability, customer confidence and regulatory compliance as well as possible opportunities, there is another reason supported by all banks. Indeed, emerging risks can be an impediment to the implementation of the strategy and the success of the objectives defined by the bank.

However, the way banks include emerging risks in their strategy differs. Indeed, in the case of Bank A, it adapts its strategy and activities according to emerging risks. As this bank wants to be more sustainable and respectful of the environment, the '17 United Nations Sustainable Development Goals' are an integral part of its activities, starting by asking for the respect of these commitments during contracts with new clients and partners. Nevertheless, the bank added that the strategy can itself induce new risks.

Moreover, the Bank A adds that it has a societal and inclusive role to play by taking into account ESG risks, which is in line with Bank B's point of view. The latter also noted that emerging risks are not a necessary reason for revising objectives and strategy.

Compared to the previous one, Bank C has a different way to consider emerging risks. Indeed, the bank starts from its strategy to evaluate possible emerging risks that can results. And justifies by saying that: *“as a financial institution you always take risk, if you do not want to take risk, you just close down your company and then you have no risk”*. The bank also adds that risks must be prioritised according to the risk management structure in place.

This is somewhat in line with the investment banking view that the bank's strategy depends on the environment in which the bank operates and added that decisions are made on the basis of emerging risks. In this way, the bank starts from its strategy to then take into account emerging risks and adapt the bank's activities (services provided to clients, product categories and investment policy) according to them.

A methodology used by the investment bank to identify the potential implications of emerging risks and trends on its business, is based on the following questions: *“how will this risk impact our activities, and can it potentially impact our financial situation and the environment where risks operate?”*. Then it gave a concrete example by specifying that the arrival of a new regulation in force requires the bank to check that it is in compliance with the bank's current process and, if necessary, to adapt the bank's *modus operandi* to meet these new regulatory requirements.

To this, *World Bank* adds that taking risks into account allows their organisation's strategy and objectives to evolve by adapting to possible threats. Their priorities are, in addition to creating value for consumers, the protection of staff, even more after the crash of the Ethiopian Airlines Boeing 737Max.

To conclude, the strategy and objectives of banks are linked to emerging risks, but not in the same ways. In some cases, the bank starts from its strategy to understand what are the possible emerging risks that this may involve and therefore prioritizes them to mitigate them. Or the bank assesses the possible emerging risks to see if they can be a brake on the objectives and adapt the strategy to these risks.

Nevertheless, banks agree that the bank's strategy may involve new risks as well as emerging risks do not always constitute a reason to review its strategy and objectives.

4. Who are the people involved in managing emerging risks?

Adapting the bank's strategy and operations to emerging risks and trends involves the collaboration of several functions within the banks, from the business lines, to the CRO, and its risk management team, to the audit and compliance functions, as well as the BofD and the Executive Committee.

Firstly, we will study the role attributed to the CRO. According to the large commercial banks interviewed, the CRO is responsible for defining the guidelines for each risk, providing the BofD with a summary of the risk appetite that the bank would ideally have and that it currently has, and the means and measures to be taken to avoid facing new risks.

In addition, only the Bank B identified the CRO as the facilitator of the (emerging) risk identification and assessment workshops. In contrast, the other commercial banks and *Euroclear Bank* identified the risk management team as the lead. To compare, the investment bank identifies the responsible of the control of each department as being responsible.

In almost all cases, the CRO is member of the management board and brings information to the executive, as well as sometimes sharing the information to the bottom-up level, in addition to the top-down level, as we will see in the section on how information is shared within the bank.

Besides, regarding the teams involved in the reporting to the CRO, the investment bank has three teams involve, which are the financial and non-financial risk teams and the compliance team. This structure can also be considered in Bank D.

Let's start by explaining the role of the risk management team, that generally includes the CRO. We find this team in all commercial banks as well as at *Euroclear Bank*.

First, the risk management team of Bank A is responsible for coordination and information sharing within the bank, and makes proposals to the management board, especially on risk appetite. This is in line with the structure of the small commercial bank, where the risk management team has various roles, such as organising risk assessment, where they play the role of facilitator, meaning being responsible for taking notes and sharing information and reporting, and possibly assigning ratings to each risks and ensuring that the business lines agree with these ratings, all with the involvement of the 'Operational Risk Management department' as well.

In comparison in the Bank C, this team is called 'Enterprise Risk Management' (ERM) or 'Integrate Risk department'. This team is composed of day-to-day managers, which are responsible for looking at the different risks that the bank face, in each country where the company is implemented, reporting back to both the BofD and to the Executive Committee of the group, as well as to the Board' body support, called 'Risk and Compliance Committee'.

However, Bank C also adds that the role of identifying risks belongs to everyone in the bank. And that it is then the ERM's role to consolidate the information received and evaluate it. This can also be seen in Bank D, which says that it discusses the identification of potential risks with all

departments, in which one person, called 'the Single Person of Contact' (SPoC) has the role of detecting and reporting risks.

Bank B, also calls this team 'ERM team'. And which is responsible for risk assessment, mainly risk mapping and scenario assessment, as well as the addition of risk within these scenarios.

The team is closely associated with the strategic risk team, whereas a distinction between these two teams exists between bank B and bank C. Regarding the latter, the strategic team is responsible for taking into account future trends that exist outside the bank and assess their potential opportunities for the bank. Such as the consideration of potential new competitors that may offer an online banking service attracting new consumers, and for which the bank must compete in order to remain competitive in the financial market.

Previously, we have seen that emerging risks were taken into account by teams more specialised in one type of risk. This is particularly visible in Bank B. Indeed, emerging risks are identified by the operational risk team, the security risk team and the financial risk team, which is responsible for risk assessment, such as scenario analysis and stress testing. Teams specialising in fraud and corruption risks are also involved at *World Bank*.

In Bank C, we can find the same situation where all the people of the group are involved and mainly the departments of each type of risk which are part of the so-called 'Risk Competence Center'.

Whereas the Bank D as well as in the investment bank, there are two teams, financial and non-financial risk teams, each with their own expertise in their fields, and whose role is to analyse emerging risks according to their sector and reporting them to the ERM team.

Regarding now the compliance department, part of the second line of defence, which is responsible for reporting to the CRO within the Bank D, and also known as the 'Regulatory Coordination team' in the investment bank. This team is responsible of the risk integration as well as the identifying of new legislation, ensuring that communication with the supervisor is done properly, that the risk management structure is properly established as well as the risk taxonomy, so that all types of risks faced by the bank are considered and managed.

In addition to the compliance and risk management teams, the commercial bank C also has a 'Peer Benchmarking' team responsible to look how other banks are doing business and their situations on the financial market, to avoid taking too many risks compared to peers.

Regarding *Euroclear Bank*, a similar role that looks at all potential new risks is in place. This function works with people in strategy, to have a broad scan on the horizon and take all possible

new risks into consideration, either treats that need to be mitigated or possible opportunities that need to be taken.

Still at *Euroclear Bank* but regarding the assessment of the risks, several teams are involved such as the 'Risk Management' team which is the facilitator, the head of strategy and the head of product management team. These teams have to report to the team called 'the Asset and Liability Committee' on the inputs collected. This latter is responsible to evaluate the impact of these risks on the balance sheet, as well as analyse the profit and loss (*cfr. P&I*).

Finally, concerning *World Bank*, this organisation also has a CRO who is notably responsible of the credit department as well as the market and counterparty department. In addition, the Chief Operational Risk Officer (CORO) of the organisation is responsible for non-financial tasks such as operational risk management, enterprise risk management, business continuity and crisis management as well as the corporate insurance and reporting.

There is a strict hierarchy inside the organisation where the 'Operational Risk Committee' needs to report to the 'Enterprise Risk Management Committee' as well as to the BofD, which main roles is to approve the risk appetite framework, and the risk management framework in general. Their decisions are based on the advice of the risk committee of the board, that has an advisory, critical and discussion role according to Bank B, either by advising the BofD on risk appetite, actions to be taken, or on stress-testing and modelling that are more technical.

Regarding its audit function, *World Bank* works very closely with it and receives advises from external consultants. External consultants that as we will see, help nearly all banks interviewed either to gain more inputs related to new risks or to assess risks. In addition, the investment bank also added that the audit team is involved in the 'Risk and Control Self-Assessment' (RCSA) exercise and that there are many exchanges between the three lines of defence.

In conclusion, emerging risk management requires the mobilisation of several teams. First of all, the CRO and its risk management team, also known as the ERM team, that plays a key role in providing the necessary elements to the BofD for the definition of the risk appetite, facilitating risk identification workshops, consolidating information from the different departments or entities and performing scenario analyses and stress testing exercises, setting up a risk management framework and integrating emerging risks, and even sharing information, both to employees and to top management.

Depending on the size of the bank, more specialised risk teams have the role of identifying risks in their categories and reporting them to the CRO. In smaller banks, there will typically be a

Financial Risk Officer, an Operational Risk Officer and, in some cases, a Compliance Risk Officer.

In addition, there are many distinctions between commercial and investment banking. The first is the role assigned to the Regulatory Compliance team, which is equivalent to the role of the Risk Management team mentioned above, but that also makes the liaison with the supervisor. Another distinction is the facilitating role given to the head of supervision in each department.

According to other teams, the Risk and Compliance Committee acts as an advisor to the BoD, and the Strategy department has been set up to assess possible risk opportunities. In addition, Bank C and *Euroclear Bank* also have functions to assess the risk management of competitors.

Finally, we have also seen that the audit function during the assessment phase is of paramount importance at the *World Bank*, although less emphasised by the other banks.

5. At what stage in the management of emerging risks do banks use external consultants?

Another key function in the management of emerging risks is that of external consultants who may be involved at different stages of the process.

All banks report using consultancy firms, and mainly the Big Four, with the exception of Bank C and *Euroclear Bank* which say that they have sufficient senior consultants with expertise. External consultants are usually called in for the identification and assessment of emerging risks.

Indeed, these consultancy firms would organise industry meetings where banks take part to discuss emerging risks they face and new legislation published by the regulator, without however revealing any confidential information. With the aim of sharing and helping each other face common risks for which they often lack knowledge. Indeed, as one bank mentioned, emerging risks impact all banks, thus knowledge on these risks is often shared between them.

Nevertheless, a first distinction between banks lies in the risks for which they use consultants and the stage in the risk management process at which they use these external companies, as you can see in appendix 16.

First, concerning Bank A, it calls on consultants to help it mainly to review their credit risk modelling, which is a task that requires expertise and for which the bank is therefore not able of establishing itself, especially as it has to meet the expectations of the legislator.

The bank adds that since these consultancy firms are costly, it tries to limit their visits and to ensure that its team is present when they come to remain a win-win situation where the

consultancy firm brings knowledge to the bank. So that the bank is independent and does not have to call on consultants for the same subjects in the future.

According to Bank B, it says that it calls on consultancy firms primarily for existing risks, but also for their expertise in cyber risks, which are emerging, evolving and becoming more and more important but whose impact is still unclear.

Finally, Bank D says it calls on these companies from time to time, to help them in their management, notably in the case of outsourcing risks such as AML and compliance risks, which were listed as hotspot risks two years ago, but no longer today, probably thanks to the expertise provided.

About the small commercial bank, it needs the help of consultancy firms more regularly than larger commercial banks. This is mainly due to the lack of experts they can hire. In addition, the bank informed me of the presence of consultants at workshops, held during the risk assessment phase, as well as for cyber-risks and modelling.

As far as the investment company is concerned, it mainly uses external consultants for new risks, in order to be able to integrate them correctly into their taxonomy. Furthermore, the bank adds that it uses consultancy firms only for the risk assessment phase. In addition to participate in industry's meeting to see how other banks act and if they have developed ways of managing risks that the bank has not thought of.

This can be compared to the *World Bank's* approach, where the audit function sometimes calls on the expertise of external consultants, in order to share expertise as well as to benchmark and compare how risks are managed by others, which could improve the organisation's process.

Finally, concerning *Euroclear Bank*, it says that it does not call on external consultants because they already have the expertise internally. But in the case where help is needed, and the bank has no doubt that it will be for ESG risks and mainly for the quantification, analysis of scenarios and to meet the 'Internal Capital Adequacy Assessment Process' (ICAAP) of the legislator, but only at the beginning of the process, after which the bank tries to stand on its own feet.

To conclude, most of the banks interviewed say that they use, or will use, consultancy firms for the management of their risks, mainly compliance and cyber risks although not the only ones. Nevertheless, not all of them use external consultants for the same stages of the risk management process, although mainly for the assessment phase.

We also note that there is a difference between the large banks that try not to call on these companies too much, hoping that the exchange of knowledge will allow them to be independent

later on, while the small commercial bank need more help as they do not always have the right people in several areas to manage all the risks they may face.

Given the divergent opinions on the stage at which banks use external consultants and on the suggestion of one of the banks interviewed, I had the opportunity to interview a consultant in risk management for financial institutions. He told me that the biggest difficulty for banks is the management of risks that are not yet mature and therefore they cannot be sure that their management process is sufficiently effective until these events fully materialise. The necessary qualities of a good risk management are therefore agility in the process it develops and accepting that risk is not easily predictable. In appendix 17, you will find a table showing the reasons why banks use external consultants in the different risk management phases.

6. How do banks collect information needed to manage emerging risks?

As we have just seen, consultancy firms organise industry meetings where banks' risk managers participate, in order to learn more about the main risks and emerging trends and to exchange their ways of doing things. However, there are other sources of information, which are listed in appendix 18, where banks can learn about emerging risks and trends that may impact them.

First, in the large commercial banks, two types of sources are used, internal and external. Let's start with the internal sources which are mainly discussions and exchanges between employees.

Indeed, Bank B carries out a broad scan with the Executive Committee every year. In addition, it carries out internal surveys, distributed to managers or experts in certain areas of the bank's activities. These experts are chosen from a wide panel of people, “ (...) typically people that have a broad view on their domain, who are involved in operational tasks an operational teams, typically it is middle management or experts in certain domains”. This allows the bank to be aware of the main risks by type of activity. It is not just a matter of the selected employees answering this questionnaire and indicating climate risks or cyber risks or other as the main risks, because that is too broad. The idea is to understand how these cyber risks, for example, are a real risk for this or that activity, is it more a risk of fraud or data leakage, etc.

Both Bank C and Bank D also emphasise the importance of internal dialogue to identify potential risks. Bank C, for example, discusses with all its departments, whether it is the treasury department, the finance department, the communications department, etc or the Chief Economist. In addition, the bank also based itself on the numerous internal reports from the different departments to centralise the necessary information in the report covering all risks, called ‘Integrated Risk Report’.

For Bank A, the second line of defence asks the first and third lines of defence on potential risks. In addition to this, the bank reads external reports to identify new societal trends and try to understand what this might mean for the bank and its strategy.

As regards the external sources mainly used by the respondent banks, they use in particular the *NBB* reports as well as the *WEF*, although the latter is more global but remains an important source for them.

Another source of information used by large commercial banks is external database, in order to benchmark the risks taken into account by other banks. Conversely, Bank C as well as the investment bank, say they do not use a database because they do not help on the identification of emerging risks. Bank D is the only one that mentions collecting data according to the priorities of the regulator and the supervisor. And both bank B and C report reading daily news as well as financial news from more specialised newspapers. Moreover, banks have the opportunity to discuss with their peers from other banks such as through informal contacts with other CROs.

Now for the small commercial bank, it says that it does not use databases such as *ORX* because it tends to think that this risk will not happen to them. The bank mainly relies on what the market or other banks say to keep itself informed of new risks it may face or waits for the public authority to tell it what risks it has to watch out for. And based on that, the bank acts.

It is also the only bank that has mentioned the work of *FEBELFIN* (*Fédération Belges des Entreprises Financière*) on various areas such as fraud, compliance or risks in general as a source of information. In addition, the small bank claims to lobby, to exchange information and participate in debates and discussions, such as on the implementation of new regulations, for example.

For optimal information gathering, the investment bank has a person in charge of each category of risk whose role is to monitor the risk and keep abreast of its evolution and then pass on the information to his/her superiors.

As regards other types of sources, the bank collects information on sectoral risks, on the basis of studies that it carries out internally or by analysing market developments to see how risks are evolving. In comparison, for ESG risks, the bank participates in industry meetings to exchange and obtain information on this type of risk.

However, the bank states that there is no special source used for emerging risks in particular but mobilises a wide range of sources. And adds that it is during this information gathering phase that it encounters the most difficulties. Indeed, the investment bank says that due to their lack of

maturity, not all the information necessary for their proper management is available, which also makes it difficult to assess them, hence the importance of sharing knowledge and know-how between banks at industry meetings.

Regarding *Euroclear Bank*, it has a person, internally, responsible for collecting information from outside the bank, taking part in industry meetings and collecting important information in the newspapers.

In addition, like commercial banks, *Euroclear Bank* takes knowledge of public databases for the collection of information such as *ORX* and goes to industry meetings, as well as calls on a Chief Economist from another Belgian bank, responsible for sharing economic information each quarter.

Moreover, *Euroclear Bank's* Risk Management team is responsible for collecting information from the outside world and consolidating it to identify potential macro trends that may influence the banks.

We have seen previously that the bank said it did not need use external consultants, having enough senior people with expertise. The bank also adds that it has people qualified in innovation and digitalisation, which is an asset for information research in these areas. Nevertheless, its main difficulty is to assess operational risks, as it says that it has never been confronted with them, and that their data is not sufficient to identify them, so the bank relies on information on operational losses from various sources.

Among the main sources of information used by *World Bank*, these are mainly external to the organisation. Furthermore, the organisation adds that the consideration of emerging risks is mainly a matter of judgement combined with observations. Indeed, according to them, databases are not able to provide data information about emerging risks, because it focuses on familiar, known risks, and that only the exchange with people and looking at what is happening in the environment can allow these risks to be taken into account.

As a result, the organization is mainly based on reports from the *WEF*, consulting firms, which it considers more to be purely marketing documents, as well as academic reports from universities or research centres and institutions such as the *EIB*, as well as discussions with entities that offer quite the same type of activities.

To conclude, we note that many of the same sources come back regardless of the type of bank. Among the external sources, we have already mentioned the collection of information from external consultants or the industry meetings they organise. In addition, banks read reports from

numerous institutions concerning the risks faced by financial institutions such as those published by the *NBB*, the *ECB* or banking associations, as well as more global risks put forward by the *WEF* or research centres and universities, in addition to reading the news.

Public database, on the other hand, is not used by three of the banks interviewed because according to them, it does not address new risks. Regarding internal sources, it is mainly a question of discussion with each department and the countries where the bank is implemented to understand the main risks by type of activity.

7. How do banks process to consider emerging risks?

Before discussing how information on risk identification is shared within banks, we will look at the process they have in place to consider emerging risks. A more detailed view by bank can be found in appendix 19 through appendix 28.

Once the information is collected, and concerning the large commercial banks, banks interviewed will generally make a list of the ten main risks they face, although Bank B only identifies five. These ten main risks are listed at the group level for bank C where, as a reminder, the CRO interviewed was the CRO of the group and not of the country where the bank is located. You will find in appendix 21, the process for managing emerging risks depending on whether it is at the group or entity level.

Once the main risks have been identified and the risk appetite defined by the BofD, these will be pooled, on the advice of the Risk Management team or the information provided by the Compliance team in the context of investment banking. Bank D defined two risk profiles, one dedicated to the banking activity and the other to the insurance activity, as well as a separate risk management for the two activities.

Based on the information collected, emerging risks will be integrated into the existing risk management framework and taxonomy. This risk taxonomy is validated each year in the investment bank but new risks can be added once a month.

As some banks have pointed out, some emerging risks involve others. Such as, for example, covid resulting in inflation risk, or increased risk of cyber-attacks. As a result, one of the questions asked to the banks was how emerging risks fit with other risk categories. The Bank A takes example of the so-called ESG risks, which it considers to be new external risks, and says that they impact credit risks, physical and transitional risks, market risks, liquidity risks and also non-financial risks. Nevertheless, in the first instance, the bank uses a silo approach where risks are assessed individually. Each team: credit risks, market risks and non-financial risks teams analyse

risks in their categories. It is only during the second phase, assessment phase where the stress testing exercises are carried out, that a holistic, collective, approach is adopted.

This is in line with the approach of Bank B that also uses a holistic approach in the assessment phase. Nevertheless, according to this bank, emerging risks would mainly be considered as operational risks. Moreover, this exercise of integrating emerging risks is a real and difficult challenge for this bank, to which the *ECB* has given a first warning, asking that the impact of these risks be assessed in financial drivers.

Regarding Bank C, it has mainly a holistic approach, where risks are integrated together and where no distinction is made between familiar risks and emerging risks. In comparison, Bank D claims to have both an individual risk approach, silo approach, as well as a collective risk approach where emerging risks, although taken into account along with traditional risks, are managed with greater importance and require more effort and for which the BofD requires a more in-depth analysis, especially for cyber and IT risks.

This silo approach combined with a holistic approach is also visible in the investment bank. Moreover, throughout the process of considering emerging risks, the bank asks itself what impact these risks may have on the bank's business, its financial position and the environment in which it operates, and then analyses the influence of these risks on the existing categories and puts in place the necessary action plans and controls to mitigate them.

Regarding the small commercial bank, it adopts a silo approach during the risk identification phase where it isolates risks and tries to identify the cause and effect of each of them. Then, for the risk assessment stage, the bank adopts a holistic approach.

As a reminder, this bank considers emerging risks as risks that have not yet materialised. So that, these risks are taken into account from the first early warning signals while continually asking what possible impacts this could have. But they find this exercise difficult, especially since these risks are new and the bank has lesser resources to put on the search of possible vulnerabilities than bigger entity. This is the reason why the company look first at what the other banks say and what the market says and after that, acts.

Euroclear Bank also says that it does not categorise emerging risks separately from the existing taxonomy. However, it has already opened a new risk category for ESG risks in the past. But now, tries to merge emerging risks with the existing taxonomy.

Moreover, the bank first adopts a silo approach where risks are considered according to clusters: economic market, geopolitics, ESG, demographic, technologic and industry shifts. Then, in the risk assessment phase, the bank adopts a holistic approach.

Also, the bank identifies risks in accordance with two different approaches depending on the duration. The first one considers more the risks they call 'top-of-mind' and those that evolve over a longer horizon.

For the first approach, these are analysed using a tool called 'European Banking Barometer' which consists of looking, once a year in June, at the main risks that the bank faces in its daily activities over the next two years. The second approach, also carried out each year towards the end of the year, is to look at the emerging events and trends taking place in the external environment. This latter exercise, carried out by the risk management team, which is responsible for gathering information and aggregating it, requires more effort than the first as it requires preparatory work for workshops with the BofD and a more in-depth analysis than the first.

Finally, *World Bank* says that it is important to look across the whole landscape and not just looking at risks in silo, in order to mitigate uncertain events as best as possible and to remain curious about any potential events. Although a more in-depth analysis of certain risks is also important.

Once the risk identification and the risk taxonomy have been completed, the next step is the risk assessment and more specifically the RCSA exercise, a notion that distinguishes the small commercial bank, which calls it 'Risk and Control Assessment'. The reason why the bank did remove the 'Self', is that it wants the risk workshops to be debated where the first and second lines of defence agree together on the risks and controls to be put in place.

This RCSA is realised once a year in the small commercial bank, where these workshops last two times four-hours, as well as in the investment bank. In comparison, Chapelle (2020, p. 4) had advised that these workshops last a maximum of three hours and take place either in the morning or at the end of the day.

This risk mapping differs among the banks interviewed, although it is often known as the probability of an event occurring on the y-axis and the degree of impact if the event occurs on the x-axis. Bank C, as can be seen in appendix 27, replaces the y-axis with a horizon axis of up to five years. The reason for this axis is that cyber risks, for example, is a risk that the bank faces on a daily basis and therefore has a very high probability of occurring but which persists in being taken into account over the long term.

In comparison, Bank D, which annually updates its risk map with the Executive Committee, proposes a vertical axis showing the degree of maturity of the bank towards the risk, and a horizontal axis showing the degree of importance of the risk. The objective of this mapping, as emphasised by bank D, is to identify the risks that could jeopardize the bank's strategy by 2023. Moreover, the risks are discussed quarterly, in this bank, with the directors of each department.

During the risk mapping phase, *Euroclear Bank* proposes four quadrants, as you can also see in appendix 27, according to the degree of uncertainty of the risk and according to the possible impact on the bank, but only for the scanning horizon. With the European Banking Barometer (EBB), i.e. top of mind exercise, risks are mapped according to the probability of the risk, which includes its uncertainty, and its severity.

In part one, we discussed the lack of structure offered to banks for the management of emerging risks and the significant number of regulations put in place by regulators and supervisors mainly on the minimum capital to be set aside and on transparency rules.

During the interviews, I asked banks if the existing regulations and structures for managing emerging risks proposed by the regulator and supervisor are sufficient for the management of these risks in their banks. Bank B replied that there were no existing structures helping to properly manage emerging risks in the banking sector but added that it is not a problem, as these risks were new to both banks and the regulator, which did not allow them to anticipate them nor propose an adequate structure.

On the other hand, Bank C says looking at emerging risks continuously, and new regulations are to be expected and that will be constantly changing, because process putting in place have not yet been tested and applied due to the fact that the regulator does not know about the real impact of these risks.

Moreover, banks agree to say that taking emerging risks into account is not easy. Besides, Bank B says looking at these risks requires thinking outside the box by going beyond what is known and to be creative and open-minded about what could happen. By the way, one of the exercises requested by the *ECB* from the banks is to imagine and be prepared for the possibility that a large-scale cyber-attack could occur and that banks' IT systems could no more be used. *World Bank* also stressed the importance of remaining open, curious and adaptable to events.

In part one, we talked about the existence of possible cognitive biases that can have a negative influence on the decision-making of action plans or on the identification and evaluation of risks. Moreover, cognitive biases are often the result of irrational judgement. This is the case for *World*

Bank, which says that it follows its instincts and accepts that certain signs put the organisation in an uncomfortable situation, but that the organisation must nevertheless accept and deal with.

Once the RCSA is realised, the quantification of scenarios can begin. Bank A, for which the detailed process of the risk assessment phase is shown in appendix 19, proposes three-four scenarios, compared to the small commercial bank that identifies between eight and fifteen, mainly covering capital, liquidity and profitability, for which the bank is gradually trying to include non-financial risks.

Moreover, Bank B indicates that it has a different procedure for quantifying scenarios depending on whether the scenarios concern familiar risks or emerging risks. Indeed, for familiar risk scenarios, the bank has a more elaborate version, which consists in transforming them into a macroeconomic driver. Whereas for emerging risks, a more simplistic version is used and for which action plans depend on a risk that can go over a time horizon of one year in addition to the action plan required over the next three years.

Regarding the investment bank, and as shown in appendix 24, it proposes two different scenarios depending on the degree of maturity of the risks. Indeed, the bank only integrates emerging risks into the risk management framework once they have been materialised. Once it is the case, the bank takes into account past events, then extrapolates the financial impact and evaluates potential future risks which are then modelled.

In the case of non-mature risks, such as climate risks, the bank will analyse, on the basis of defined parameters, the potential decrease in value or income that could be generated by the potential risks, based in particular on research from academic or institutional sources.

The risk assessment phase also includes stress testing exercises such as ICAAP and ILAAP, performed in April and recalculated monthly and quarterly within the small commercial bank, to be presented to the Executive Committee. However, as these exercises are included in the familiar risk exercises, I did not go further in the interview.

Once these scenarios have been quantified and modelled, comes the risk mitigation step. During this phase, Bank B specifies that emerging risks are not managed in the same time frame as familiar risks, as the reason for their mitigation differs. Indeed, Bank B justifies by saying that climate and transitional risks must be taken into account, not because they are urgent, but because if the bank does not take them into account now, it will not do so in thirty years. Regarding cyber risks, they also must be considered now because the bank is facing them on a daily basis. Thus, action plans are defined each year for the next three to five years.

During this stage, the implementation of KRIs is important. Bank B takes these KRIs from databases or the one published by other competitors. As emerging risks are often not materialised and cannot be based on historical data, and are therefore difficult to evaluate in monetary terms, the investment bank and Bank A said they used qualitative KRIs. Only *Euroclear Bank* and *World Bank* says they don't use KRIs.

These KRIs are evaluated monthly or quarterly by Bank C. The investment bank also performs a check which can be weekly, monthly or quarterly depending on the type of risks involved. And adds that KRIs are defined both at the group level and at the level of each entity or activity, which is also the case for the small commercial bank.

Finally, regarding the *World Bank*, although it is not subject to any regulations, the organisation behaves as such and implements its own rules based on the regulations in force.

A key difference between this organisation and the other banks interviewed is in the people involved in risk management and the procedure to manage risks. Indeed, the organisation has a dedicated crisis management team in each country that has procedures in place in case a risk occurs. And if a crisis happens, the Chief Risk Operational Officer and the CEO make the decisions related to this risk through the Chief Operational Risk Committee.

Finally, once the crisis is over, the organisation always takes a double look, like *Euroclear Bank*, one of which is turned to the past to identify potential management errors so as not to make them again in the future.

To conclude concerning the way emerging risks fit with the so-called traditional risk categories, we note that banks interviewed adopt the same approach which is a combination of a silo approach and a holistic approach and by integrating these risks into the existing risk taxonomy.

Moreover, taking emerging risks into account is not easy and sometimes requires making judgments about possible events by being curious and scanning the environment. It is a continuous process where many cognitive biases can appear due to the uncertain, ambiguous, and complex nature of risks.

Among the distinctions between banks is the way risks are mapped, KRIs defining, and information shared, it depends on whether the bank is a group composed of different legal entities/countries or whether it has a banking activity and an insurance activity. In both cases, banks perform the exercises independently for each entity/activity.

Regarding the analysis of scenarios, it is done differently according to interviewees. Indeed, whereas the investment bank carries out the exercise according to the degree of maturity of

emerging risks, Bank B uses two versions of scenarios: a simplistic one for emerging risks and a more sophisticated for familiar risks.

Concerning the risk control phase and more particularly when setting up indicators, we have seen that Bank A and the investment bank used qualitative indicators to cope with the lack of information necessary for the proper management of these risks. In addition, there are many similarities between *Euroclear Bank* and the *World Bank*, whether it is the lack of use of indicators or a backward- and forward-looking approaches that allows the organisation to be aware of past risk management mistakes so as not to make them again.

Regarding the frequency of reporting to the BofD and the Executive Committee, most banks indicated that it depended on the risk, but it varied from semi-annually to eight times a year. It is less common for information to be shared with employees, but if this is the case, question and answer (Q&A) sessions or internal report distribution can be set up.

8. How is information on emerging risks shared within banks?

Once the information has been collected and the risks are identified, and assessed, let's talk about the reporting of the information within the bank. The reporting can be done through both a top-down approach, where the information is shared from top to bottom of the hierarchy which is the different departments and employees of the bank; and a bottom-up approach, from the various business lines to the top management.

This sharing of information, a summary of which can be found in appendix 28, is broken down into different reports depending on the approach to which they are addressed but also according to different distribution channels.

Let's start by understanding the different risk reports shared by large commercial banks with top management. In the case of Bank A, the CRO is responsible for issuing a quarterly report on the main risks faced by the bank during the previous quarter and their description, indicating their possible evolution for the next quarter and whether they could be mitigated and finally proposing recommendations. This report was distributed to the board members in the form of a five-six slides power-point.

Bank B also conducts numerous updates through presentations to superiors on the main risks it faces. Risks are not always reported with the same frequency, depending on the risk and its severity. Indeed, the bank said that it reported cyber risks every six months to the BofD and that typically these were risks for which regular updates on the possible impact on the bank are required.

Bank C, on the other hand, shares numerous reports with their top management that they meet ten times per year. The first is what they call a 'Health Check', which is included in the 'Integrated Risk Report' and reported to the BofD and to the Executive Committee eight times a year, and which shows the status of the indicators of all risks, and where the bank stands in terms of capital and performance.

In addition, once a year, a report called 'Risk Scan' carried out during the second-third quarter, contains the risk map with the ten main risks facing the group. And in addition to this, another report, called 'Risk Signal', is shared eight times a year with the senior general managers and the CRO of the group and then discussed with the Executive Committee.

Finally, a fourth report shared twice a year at the top of the hierarchy concerns the risks identified in the products offered by the bank, which is called the 'New and Active Product Process' (NAPP). Which consists of the identification of risks for each existing or new product proposed, and it involves different departments such as the IT department, the compliance department, etc. These different departments analyse together whether there are any possible problems with a product that could lead to new risks, and how they can respond. This report is then sent to the BofD and the Executive board twice a year.

Bank C also says that the reporting depends on the type of risks and, if necessary, the information can be reported to the BofD and the Executive Committee directly.

Regarding Bank D, it did not specify the sharing of reports with the Board. But instead, said that it conducts what is calls 'tutorials', in addition to usual meetings. These meetings, which are not mandatory, allows the BofD to ask additional questions about the risks the bank faces and can go more in-depth in case of misunderstandings about one of the risks. The regular reporting takes place every quarter where risk appetite metrics, limits and then the whole risk appetite framework are cascading. In addition, every month the information can be reported in the specialised committees.

Now about the person responsible for sharing information, within the company and with the board, it is done, in all commercial banks interviewed, by the '(Enterprise) Risk Management team'. But we will see that it is only valid for reporting at the top of the hierarchy for bank D, which has other people responsible for reporting down the hierarchy.

Bank C also adds that it is the CRO who ensures that information is given to the various members of the executive and the rest of the group. Meaning that the information is shared with the CROs in each country where the bank operates, who in turn share the information within their country.

Turning now to the way how the information is shared with the employees in these banks, Bank D explains that they have what they call 'CRO talk' where all employees can join the meeting and ask questions, about emerging risks for example.

In comparison, Bank B uses two distribution channels to share information among their employees: an internal intranet, where information is shared in order to allow employees to be aware of new risks, but they regret that not all employees go on it. And there is also an e-learning system, also accessible to all employees, on specific topics such as climate change, or phishing.

In comparison, Bank C also uses platforms where employees can share information both within and between departments, such as internal social network where employees share information, comment on it, and more importantly create communities of shared ideas, thoughts, and observations. The initiative for this platform came from the business functions, not from the risk function.

For Bank D, in the absence of an intranet, and as we said previously, they have a person within each department called a Single Person of Contact (SPoC) who is responsible for sharing information within their department.

Finally, a last report put forward by Bank A and C concerns a report requested by the regulator. Bank A called it 'Effective Leading' where the main risks the bank faces are discussed. While Bank C called it 'Risk Signals' and it concerns either a specific risk, or a combination of risks, or even all the risks, whether internal or external, such as new regulatory risks, that the bank wants to describe to the top management eight times a year.

Regarding the small commercial bank, this one says that it has mainly an approach where reporting is only upwards to the hierarchy and that it does not share the main emerging risks it faces with employees. The reason is that the bank does not find it engaging. Although it does answer employees' questions, if they have any, but when sharing information with employees, it is mainly about the bank's results and strategy, the employee satisfaction barometer and gender diversity.

In comparison, the investment bank shares information both, to the top and to the bottom, through the compliance team at least once a quarter. Regarding information shared to the top, it is through a risk dashboard, which has a dedicated emerging risks category, listing emerging threats and factors, and which is shared with the Executive Committee and the BofD.

In addition to that, there is a top-down approach, where new risks are also communicated to the different departments, in addition to a discussion with the first line of defence. This takes place

monthly or quarterly depending on the type of business where the new risks are discussed, but it is part of a meeting where not only the new risks are discussed, but the whole set of risks and controls that the line of business faces. Indeed, emerging risks are not the subject of a particular meeting or report but discussed in the risk and control process or included in the general report.

In the case of *Euroclear Bank*, the information is shared by the bank's risk management team with both the group, and more specifically the group CRO and the bank's CEO. This reporting is realised by a dedicated meeting where information is shared via slides and where discussion is actively carried out with experienced board members, in order to compare ideas and a feedback is given on the preparatory work carried out.

Just like the small commercial bank, the information is mainly passed on to the hierarchy, as the information is not shared with all employees, although it is shared with a senior committee called the 'Asset and Liability Committee'. This committee is composed of people responsible for the balance sheet and to calculate the p&l.

Finally, regarding *World Bank*, the information is mainly shared at the highest level of the hierarchy each quarter, for which the management team is responsible, which includes the head of the operation in the insurance function and the head of the business continuity management and crisis management function, i.e. the CORO. The latter reports, along with the rest of the 'Operational Risk Committee', to the highest-level risk committee, meaning the 'Enterprise Risk Committee', which is chaired by the Managing Director, and to the BofD. The reason why there is not only one person responsible for sharing information is to avoid cognitive biases by using dialogue between the people involved, in order to best deal with all the risks that one person alone is not always able to identify and analyse.

9. General conclusion

As a general conclusion, among the main differences in risk management between these banks are the following.

Emerging risks, although called hotspot risks, are known risks which have not yet materialised and whose structure does not always allow them to be properly managed by the banks. They are subject of an approach which is both silo-based, during the identification phase; and holistic-based, during the assessment phase.

Banks interviewed faced mainly the same emerging risks: cyber risks, climate risks, compliance risks, cyber and IT risks, interest risks and business risks. These risks are part of the traditional risk taxonomy, and their causes must be clearly identified, as one emerging risk may lead to

another. Furthermore, these risks are fully integrated into the banks' strategy and objectives which are reviewed accordingly.

Among the main distinctions between the banks interviewed, we notice: the difference between large and small structures. The latter, having fewer qualified staff, are more likely to use consultancy firms. Secondly, the large structures will have more risk management functions specialised by type of risk, whereas in the small structures there is generally only a CFO, COO and a CRO.

Although, the role of facilitator is often given to the CRO and the risk management team. Another distinction is the phase during which banks ask for help from external firms.

Moreover, the focus of risk mapping or the use of indicators in the control phase are also different, some banks not using any, others relying solely on qualitative indicators.

Regarding the way information on these risks is discussed, it is usually between the three lines of defence. In the case of groups, it is first reported at local level before being reported at group level. We have also seen that risks are reported mainly to BofD, whose frequency depends on the risk, and more rarely reported to employees.

Finally, as financial regulator banks are not regulated, they act as such and have set up a risk management structure with different people involved compared to the other banks.

In the following pages, recommendations drafted by myself and based on a comparison between the literature review, the bank interviews and my own experience are proposed. These recommendations are intended to help banks in their management of emerging risks, which, due to their uncertain and ambiguous nature, as well as the fact that these risks have not yet materialised or are evolving, are difficult for banks to grasp.

Indeed, *World Bank* said that the difficulty in taking emerging risks into account is in the judgement that is made, as the organisation is mainly judgemental about these types of risks. This is in line with the vision of the Bank B which is mainly judgemental about whether or not to include some emerging risks in the scenario quantification exercise and the stress testing phase.

Moreover, the bank adds that taking emerging risks into account requires going beyond what is known and keeping an open mind to what is happening in the external environment and looking outside the box.

In comparison, for Bank C it is precisely the capacity of events to evolve in the external environment, or possible new regulations that represents a real difficulty. While for Bank D, the

challenge lies in the regular identification of these risks and in the implementation of action plans, in order to mitigate them as well as possible.

Finally, for *Euroclear Bank*, it is mainly during the assessment phase that the risk lies, as the modelling carried out is not always sufficient to take into account the severity of the event and the probability that it will occur. Not forgetting the systemic impact of these risks on the entire banking sector when it materialises. This is in line with the main challenge facing investment bank when dealing with emerging risks, because they are not yet mature and difficult to anticipate.

Corpus of good practices

1. Emerging risks identification

As indicated by the banks interviewed, the way emerging risks are managing is a continuously process of risk identification, assessment, mitigation, control and reporting.

The first step, the identification of emerging risks, requires banks to scan the environment continuously to identify possible new risks and their evolution over time. This broad scan exercise, which can also be called ‘horizon scanning’, is generally carried out once a year by banks.

However, in view of the recent news with many disastrous events related to climate change and the increase in cyber-attacks and their changing nature, as digitalisation and working from home becomes more widespread, I advise banks to be even more vigilant to all potential events and carry out this horizon scanning exercise semi-annually.

In addition to this broad scan, I advise banks to perform the same exercise but internally, also once a year. This exercise would identify risks related to the bank's objectives and strategy as well as to its product and service offerings.

Regarding the people involved during the identification phase, it would be interesting for banks to set up functions by type of risk: compliance and regulatory, liquidity, ESG, cyber security and IT security, who report directly to the CRO of the bank. Thus, risks are managed centrally by a CRO and its risk management team after having been identified and assessed in silo by individuals responsible for each type of risk.

However, this is not possible for small banks, in which case a financial risk manager and a non-financial risk manager, who can work together with the CRO may be a solution. In addition to the help of external consultants or a Chief Economist from another bank who would come and present the possible risks that banks may face.

One way for banks to ensure that all emerging risks have been identified is to compare their data with databases such as *ORX*, during the identification phase of emerging risks. This to ensure that no risks that could impact the bank and the banking sector in general have been overlooked.

In addition to benchmarking their data, banks can also rely on reports from the *WEF*, *BCE* or by working groups such as *FEBELFIN* and documents from consultancy firms, highlighting key

emerging trends and drivers of emerging risks to ensure that banks are aware of all the emerging risks they may face.

Regarding the identification and analysis of new trends in the external environment, this can be done by the strategy team in large banks, in order to also identify possible new opportunities for the bank, as emerging risks are not only threats.

In the case of small organisations, one person can play this role, or it may be interesting to set up an internal social network or intranet link where employees can post about new risks they have identified or read about in the news.

Another idea, observed during the interviews, is that banks can compare their situations with those of others. This can be done during industry meetings organised by consulting firms or during more or less informal discussions between CROs of banks. As emerging risks impact all banks unintentionally, and the impact on one can have adverse effects on others as in the case of cyber-attacks, cooperation is essential. The idea is to share information on what are the main emerging risks the sector faced, how to manage emerging risks, and where banks can share their ways of doing things that some other banks would not have thought of, without disclosing confidential information.

In addition to this, a team or a single person can also be appointed to carry out benchmarking among the bank's competitors, in order to identify risks that the bank has not yet taken into account or to look at whether any banks have a risk management system that could be applied to strengthen the current structure of the other.

Finally, the arrival of a Chief Economist from another bank for the one that doesn't have, and I am thinking in particular of small commercial banks that have less in-house expertise than large banks, could be an asset that would allow them to have a global vision of the main emerging risks and their economic and financial impact on the banking sector. As emerging risks are mainly the same within the sector and banks are interdependent, this information gathering and risk assessment solutions can be a real asset if they are well taken into account, especially for small banks that act more as followers by telling themselves that these risks will not happen to them, and wait to see how the big banks act, to act in their turn.

For groups with banks in different countries, I suggest that they organise quarterly meetings between the group CRO and the local CROs to discuss potential risks that could impact the group, and in any case before each RCSA exercise with reporting to the BofD and the Executive Committee. Indeed, in some cases, such as war or terrorist threats, drought, countries suffering

from fires, these risks become so important that they must be considered at the group level because they can result in significant economic losses or threats on other countries.

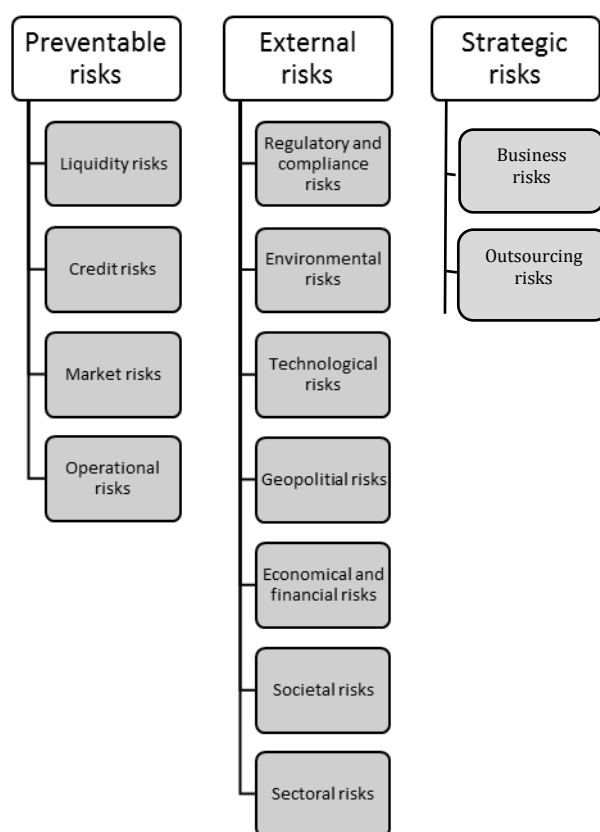
2. Emerging risks assessment

Let's move on to the second phase of managing emerging risks called assessment. In this phase, emerging risks are mainly integrated into the familiar risk taxonomy and are not categorised separately.

Nevertheless, each bank makes its risk taxonomy as it wants, whether by classifying risks into two types: financial and non-financial, or by deepening the categories: liquidity, market, credit, operational and business risks.

In order to have a taxonomy of risks where the classification of emerging risks is not confusing, I am thinking in particular to one of the banks interviewed who categorised climate risks as financial risks, and with the publication of the *Basel Committee's* report on climate-related financial risks, it could, in the future, become difficult for banks to know whether climate risks are financial or non-financial risks.

I propose the following risk taxonomy, in which emerging risks would be categorised mainly as external and strategic risks, and where familiar risks would be considered as preventable risks:



Moreover, we saw in part one and two that emerging risks can also be categorised according to their degree of knowledge: known, known-unknown, unknown and unknown-unknown risks. Nevertheless, I would not advise banks to attach too much importance to such a categorisation for the following reasons.

Firstly, emerging risks evolve in the environment. And therefore, while they could be categorised as known risks, they may become risks that materialise in an unpredictable way. I am thinking notably of risks related to climate change, which materialise currently in the form of forest fires, rising temperatures, rising water levels, etc. But in the future, new way of materialisation may appear, as said by Bank C: *"(...) the big impact is still to come but we still see very small impacts (...)"*.

Secondly, we have also seen that these risks are increasing in intensity and severity and therefore, although they are known, they cannot be properly managed by the risk management structure that banks have. This is particularly the case for cyber risks, which banks continually face but continue to consider as emerging risks, despite mitigation and preventive control procedures.

Therefore, these risks need to be managed continuously, depending on their type. But whether they are known or not, we have seen that the banks do not have a structure mature enough to take them into account. Nevertheless, and as said before, banks can carry out an assessment and control more regularly for risks qualified as less mature in order to identify at best their possible consequences.

Beyond the organisational aspect, the management of emerging risks also requires a good mobilisation of more technical tools.

Indeed, during this assessment phase, risks can be categorised and analysed on the basis of a PESTEL analysis (political-economic-social-technologies-environmental-legal), to understand what the risk consists of, how its trend is moving, and the possible consequences on other types of risk. This tool is even more important as it allows to assess possible risks over the long term, and as Bank C indicates, emerging risks have: *"little to no impact in the short term, potentially big impact in the longer term"*. This analysis should ideally be updated semi-annually, to cope with changing risks and new trends in the environment.

Emerging risks should be assessed as soon as the first warning signals appear. Indeed, due to the uncertain and ambiguous character of the emerging risk and its evolution over time, controls and action plans need to be put in place from the first signals and be reviewed in the long term after each event has taken place. Especially as the severity of these emerging risks may be more

frequent, whether it be the risks linked to climate change which will be increasingly frequent and significant, or cyber risks which are evolving in nature and in their complexity.

In this second phase, emerging risks can be approached in two ways: by combining a silo approach with a holistic approach. Especially since the risks are interdependent and have impact on other risks categories. Indeed, the covid pandemic, considered to be an emerging societal risk, will have led to an increase in cyber-attacks as we have seen, put many sectors out of business, although the banking sector has well survived, thanks to the digitalisation of its services and state aid for their clients.

Once the BofD has decided on the bank's risk appetite, on the advice of the CRO, limits and risk profile, as well as the bank's strategy, the risk mapping can begin. Nevertheless, I would like to point out that it is important when banks set their risk appetites to accept that a zero tolerance of emerging risks is not possible, because they are unpredictable.

The risk mapping, which is called 'Risk and Control Self-Assessment' (RCSA) has to be done once a year, based generally on the top ten risks to which the bank is exposed, and which may have an impact on the bank. The facilitator is usually the risk management team and the CRO. I advise them to agree on the terms and on the definition and characteristics of the axes before the exercise.

Indeed, during the interviews, we noted that different axes were proposed. Let's go through them one by one.

One of the banks said that it used an axis of maturity of the bank to face the risks. I would not advise the use of such an axis because, as many banks have told me, emerging risks are risks for which the bank's structure is not mature enough to take them into account. Especially as these risks are so ambiguous, uncertain and evolving over time, not to mention the increasing number of directives and regulations that banks have to respond to, which requires a constant renewal of the risk management structure.

Regarding an axis related to uncertainty, again, I do not advise this, given the uncertain nature of risk and their evolution over time, making them even more uncertain. Concerning the time horizon axis, I do not advise it neither because, as we have seen before, these risks take place over a wide time horizon. But, I advise banks to carry out a risk map for a period of one year and another for a period of three years, like their financial plan.

Moreover, the uncertainty can be taken into account more in a third dimension, mentioning the fact that the risk has to be re-evaluated regularly, in order to adjust the measures in place to mitigate it.

We also saw that a risk velocity axis was possible, but again, I do not advise this, as the following main emerging risks: cyber risks, are happening on a daily basis, and climate risks happened more and more regularly, and both are increasing in severity and numbers over the years. The inclusion of such an axis would require the banks to be constantly revised.

To conclude, a good method that I advise banks is creating a risks map with the probability of the risk occurring or its possible impact on the y-axis and the severity of the risk or the degree of possible impact on the x-axis.

Identifying risks and setting strategy and objectives within the bank is a two-way process. Indeed, once the strategy and objectives have been decided, only those risks that may impact the bank and the achievement of its objectives and strategy should be considered. Then, on the basis of the assessment made, the BofD should be recommended or discouraged, depending on the risk appetite decided beforehand, if the strategy and objectives are not too risky and, if necessary, reviewed. A question that risk managers, as well as top management, should constantly ask themselves and keep in mind is: "*What if...?*" or "*What could make it that we do not realise it?*".

Moreover, regarding the quantification of scenarios, banks are advised to assess the emerging risk scenarios before and during the contract with a third party, as well as according to the bank's strategy and objectives.

This quantification of scenarios is done by type of risk and can be assessed in terms of possible economic losses, customer losses, losses in terms of the value of the assets the bank holds, etc. Such potential losses are multiplied by the probability of occurrence of the risks. As we have seen previously, emerging risks increase each year in number and severity. So, by using historical available references augmented by a coefficient that reflects the increase, we obtain the amount of possible profit or loss. This one is added to the amount of regulatory capital imposed on banks.

In addition, a clarification I would like to make, and that you can find in appendix 29, after having listened to many consultants, particularly during my internship with a consultancy firm specialising in operational risk management, sharing with me their way of calculating risks. I note that many of them multiply the probability of occurrence with the possible impact.

Indeed, and as you can see on this appendix where I realized a simulation of quantification of the risks according to my own judgment and which deduces that if a risk is calculated by multiplying

the probability of occurrence and the degree of potential impact, this would mean that cyber-attacks and risks related to climate change are more important than the risks of pandemics, terrorist attacks, airplane crashes and new regulations for banks. But the organizational and economic effects are not the same for banks.

This exercise should be carried out once a year with an average of ten scenarios, which may be less for smaller organisations. Nevertheless, I would advise banks to carry out an assessment of certain types of risks more frequently, such as cyber risks, which take place on a daily basis. For these, as well as for climate risks, which have been on the rise for some time, I suggest that banks discuss them at least quarterly, especially during period of crisis or big impact.

Moreover, it was also seen in interviews that banks carried out two types of scenarios: for risks that have materialized and for risks that have not yet materialized and according to financial and non-financial risks. First of all, I advise banks, when creating scenarios, to make a distinction between familiar, and emerging risks. The latter can also be integrated into the analysis of current risks once they have materialized, such as cyber risks, risks that occur daily.

The reason for this distinction lies in the fact that these risks are still too uncertain and ambiguous to be able to calculate their financial impact, in monetary terms, on the bank, and that we do not fully know when they may materialize.

As for another possible distinction between so-called financial emerging risks and non-financial emerging risks, I leave that to the judgement of the bank.

In addition, for banks with both insurance and banking activities, it is preferable that the bank provides different scenarios for each activity. Indeed, as we have seen in part two, banks will be more impacted by the risks of fraud or money laundering, and insurance can be more impacted by the risks related to climate change, to give some examples.

The quantification phase of the scenarios, should take the form of a workshop, lasting ideally two four-hour sessions, and ideally over two days to allow the teams involved to come with more distance and time to reflect on what was done the day before.

A critical point in this phase is the possible cognitive biases that may result. To avoid these cognitive biases, it is important that those involved in the management of emerging risks are aware of them and put in place an action plan to combat them, such as bringing in external consultants to workshops, to challenge the discussions and positions of those involved in risk identification and assessment.

In addition, the fact that these workshops have been the subject of a prior individual and anonymous survey on the possible risks and their impact can also reduce the risk of cognitive bias. Especially since emerging risks are risks where historical data is not sufficient to manage them, it is important that people are aware that relying on events they know about is an obstacle to implementing action plans and that they need to be open-minded and creative about potential risks or consequences that may impact the bank's survival.

One way to ensure that employees are curious and able to be open-minded is to hire people who are interested in daily activities of the bank and have sufficient knowledge and involvement in new regulations imposed by the regulator, while being able to import a summary of the information to the BofD by getting to the point and able to explain it without using overly technical terms. In smaller organisations, hiring people with this expertise may be difficult, in which case the use of external consultants may be interesting during the assessment phase.

Moreover, it is important that when external consultants are present in the bank and share their knowledge, the bank risk management staff is also present. Indeed, hiring external consultants is costly for banks. And as some risks may be of uncertain duration and can come back, the transfer of knowledge from external consultant to internal risk management team and giving them the capacity to manage risks on their own is essential. Except in the case of banks which may not have the benefit of qualified staff in all areas to manage risks themselves and who need more presence of consultants.

Once an event has materialized, I advise banks to review their risk management process to identify possible errors or failures and to constantly strengthen their structure against new threats. While forward-looking, without taking too much account of historical data, as risks evolve over time, and increase in intensity and frequency keeping a backward look can lead to a cognitive bias that must be avoided.

During this risk assessment phase, banks are led to carry out exercises called ICAAP, ILAAP which are stress testing exercises, and notably requested by the regulator and the supervisor but for which I will not go into more detail, not being differently managed to emerging risks but to risks in general.

3. Emerging risks mitigation

Now let's move on to the third step in the management of emerging risks, which is the mitigation of these risks through the implementation of action plans and controls.

Since emerging risks do not evolve over the same time horizon, I advise banks to take mitigating measures and action plans: one in a short term with a time horizon of one year, and another one with a longer term of a three years' time horizon.

Moreover, these action plans would be reviewed regularly, after each incident because the risks do not occur on the same timescale. Indeed, cyber risks are part of the daily risks of banks, and they must be prepared to face a possible massive attack at any time preventing their access to servers and IT services. In comparison, climate risks have impacts that are already visible today but for which the big impact is still to come.

4. Emerging risks monitoring

In large organizations, the CRO of each function: IT, compliance, liquidity, or more generally COO and CFO if the structure does not allow for a CRO per function, is responsible for the implementation of effective controls and monitoring of risks.

This fourth part, which precedes risk reporting, is the stage during which the KRIs are identified. First of all, since emerging risks cannot be relied upon for historical data, which can then be extrapolated into financial data, KRIs will most often be in a qualitative and not quantitative form, this last form can be done once emerging risks become mature risks.

In the case of a large group, it is better for the bank to propose KRIs at the group level, as well as for each legal entity or country, as these are not impacted in the same way by risks. For example, regarding climate change, it depends on whether the country is on the coast and subject to rising sea levels, or in an area prone to severe drought or fires). In addition, there are also indicators based on the type of activity, other than banking or insurance, and on whether partnerships are made with third parties, for the same reasons as indicators by country.

Finally, depending on the type of risk, these KRIs should be reviewed more or less regularly, ideally once a month or quarter.

5. Emerging risks reporting

Finally, comes the last step which I consider to be risk reporting. During this stage, there are two types of reporting that I advise banks to do: a reporting to the BofD members and to the Executive Committee, as well as a reporting to business lines and employees.

Regarding the reporting to the top management, once again, I recommend that it is done according to the type of risk, generally semi-annually or even quarterly in order to ensure that top management is aware of the importance of taking these risks into account when defining the

bank's strategy and objective. Nevertheless, it is important that the CRO, and the risk management team in general, are able to report immediately to the C-suite in the event of a crisis so that immediate action can be taken at group level.

The reporting can be done through a visual presentation, such by PowerPoint slides, and by the CRO and the risk management team in general. In addition, a pdf document can be shared to the BofD and Executive Committee following the presentation, listing the main risks faced by the bank and their possible impact on the bank's business and finances. The objective here is also not to overwhelm the top management with technical terms and documentations with an incalculable number of pages. But the information needs to be understandable for non-experienced people in risk management and does not take too much time for the Executive members and the BofD to read it.

I would also recommend that in the report issued to the management and the executive, an explanatory note is written on how the risk assessment was calculated as a whole and on how the different types of risks faced by the bank as well as the main emerging trends, but only those that can have an impact on the bank's objectives and influence decision making. It is also important in these reports that board members understand the financial impact of these risks on the bank and its strategy.

In addition, for a good involvement of the board in risk management, I suggest to banks to let the Board members express themselves on possible ideas and recommendations they would have as well.

In order to best guide the Board in its decisions and recommendations, the establishment of a Risk Committee, also called Risk and Compliance Committee, is essential. This committee plays an advisory, critical and discussion role. Its purpose is to advise the BofD on risk appetite, the impact of stress testing, criticism of the action plans to be adopted and more in-depth discussion of certain hot topics towards what has been previously done by the risk management team.

Nevertheless, the reporting of emerging risks does not have to be the subject of a specialised meeting with the BofD and can be part of a meeting where the risks are discussed as a whole since emerging risks are taken into account in the traditional risk categories.

Finally, in addition to sharing information with the top, it is also important that information be shared with departments and functions that may be impacted by these risks as well as employees who wish to do so.

One way to share this information with the bottom is, for the CRO, to organise virtual or presentational sessions once or twice a year, where employees can ask questions and interact about possible emerging risks. Another way is to publish an internal report on the main emerging risks and their possible impact on banks, which is also easily understandable to people not qualified in risk management and not too time consuming.

In the case of groups with entities in various countries, it seems important that information on emerging risks is also shared with them via the transfer of information from the group CRO to the local CROs, who are then responsible for sharing the information within their entity with the same means as mentioned above.

In general, risk communication is as important as the management of risks. Communication is often an integral part of the bank's culture. In addition, investors, customers, regulators and all bank stakeholders increasingly expect transparency and ethics from banks. Indeed, as some banks told me during the interviews, they have a societal role to play and must be inclusive.

In addition, a clear and concise communication and information sharing, between the various bodies involved in risk management is important. In other words, between the three lines of defence, between the CRO and his team, and between the CRO and the BofD as well as the Executive Committee. Where a corporate culture of transparency is ideal so that every employee knows what the main risks their company is facing and can participate in the collection of these risks.

6. More generally

In order to stimulate employees as well as to involve them in the bank's activities, it can be interesting that once a year employees take part in group workshops. The groups would be composed of a limited number of employees, depending on the size of the bank, coming from different departments of the bank, and would be given an emerging theme to analyse and respond to. Such a workshop, facilitated by the risk management or risk compliance team, allows for both team building and the provision of input that the risk management team may not have previously considered.

Concerning the role of the CRO in general, I would also like to add the importance that the CRO can play as an advisor in the adoption of the bank's strategy. Indeed, as the CRO is aware of the risks that banks face and has the expertise to manage them, it is important that he/she can advise the top management when making strategic decisions such as outsourcing or when having a contract with a third party, considering the possible threats of such decisions.

In addition, a role that should be associated with the CRO and that we have not yet identified is to ensure that the (emerging) risk management framework is well implemented. At group level, it is the function of the local CRO to ensure that this framework is well implemented in its entity. Finally, the CRO is also responsible for ensuring that the risk taxonomy is reviewed at least once a year and that all emerging risks are properly integrated into it.

The analysis of emerging risks is an ongoing process, with no real fixed date and limited timeframe. Thus, it is important to encourage and stimulate the curiosity of those involved in managing these risks through non-financial rewards. This is especially important during the risk assessment phase, which is rarely easy given the uncertain and complex nature of these risks, to ensure that the people whose job is to manage these risks, are recognized and that they can continue to carry out their tasks in good conditions.

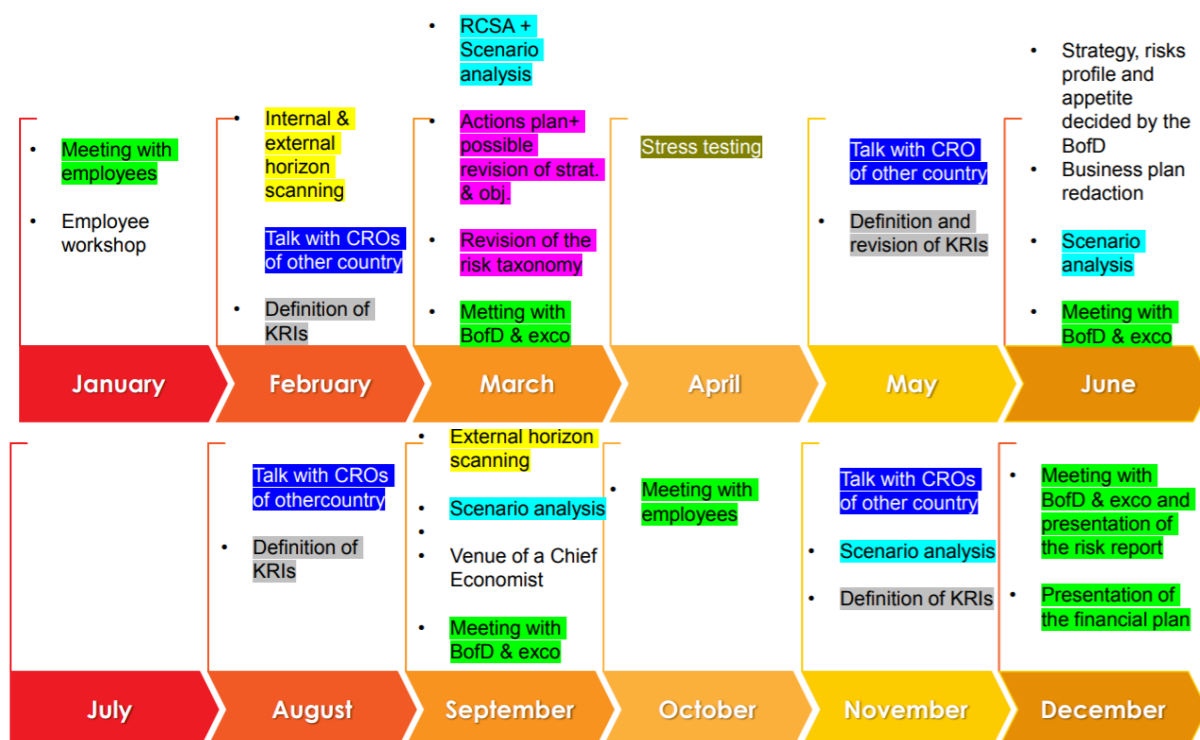
Examples of non-financial rewards could be extra holiday days, the offer of an electric bike, help with paying for a car, help with pensions, offers to take part in training, etc. as proposed in the 'cafeteria plan'.

Regarding financial regulator banks such as *World Bank*, and for optimal management of emerging risks, I advise them to act as if they were regulated, even though they are not, and to perform the same steps and recommendations as above.

Moreover, it is also essential that the organisation reviews its crisis management strategy after any event has taken place, to ensure that it is continuously improved, while being adapted to the main emerging risks per country, or by type of country facing the same type of risk.

Indeed, I advise financial regulator banks to adopt a country risk assessment, on the advice of the crisis management team in each country, which will then be fed back to the group's CRO and assessed by the Operational Risk Committee.

Above you will find a proposed timeline for the management of emerging risks in banks. To this, I would like to add some clarifications.



First, it is important to remember that the risk management process and action plans should be reviewed after each event and therefore not added in the timeline.

I propose that the meeting with the CROs of the different entities, that make up the group, is done in May. The purpose of this meeting is to ensure that the action plans are also defined within each entity and to get feedback from them on the implementation of the management of these risks.

I would also like to add the implementation of the scenario analysis exercise after the call with the CROs, for groups, as this way the risks can be reviewed depending on whether one or the other needs to be escalated to the group level.

Regarding the choice of the scanning horizon, this is ideally done a second time in September as institutions such as the *CRO Forum*, *McKinsey* and others tend to publish their emerging risk analysis around June-July and these are necessary for banks to properly identify all potential emerging risks. Especially as they will be the basis for the risk report to be presented to the BofD in December.

Finally, I also insist on the importance that the KRIs, depending on the type of risks, be reviewed at least quarterly or monthly.

Conclusion

We have seen that the financial crisis of 2008 as well as the recent events related to the covid crisis and climate change have had major effects on the banking sector.

The regulator, as well as banks, have a perception but no precise knowledge of these so-called emerging risks, nor do they know how severe they will be or when they will materialise.

This thesis aimed to provide banks with tools and recommendations for emerging risk management, according to the four key stages of risk management. In the risk identification phase, we have seen the importance of looking forward and taking risks into account from various assumptions and from the first early warning signals. During this phase, it is important that banks read reports published by certain institutions and organisations on key emerging risks and trends and discuss with their peers to ensure that all risks are considered.

Secondly, regarding the risk assessment phase, we have seen that it is interesting, in the first instance, to adopt a silo approach, to identify the causes of the risk. Then, the risks are assessed with a holistic, collective, approach where they are integrated into the traditional risk taxonomy. This is followed by risk mapping and scenario quantification, where the risk management team supervises and carries out, by avoiding possible cognitive biases. Finally, this stage ends with the stress testing exercise.

The third step concerns the implementation of action plans to mitigate the risks, which must be reviewed after the occurrence of each event. The control phase, on the other hand, is based on the implementation of qualitative risk indicators to ensure that these risks do not exceed the appetite set by the bank's Board of Directors.

However, these steps differ according to the type and size of the bank. Whether is it in relation to the teams involved, the use of external consultants, the relationship between the Chief Risk Officer and its top management, the way in which risks are prioritised, etc.

In addition, there is also the reporting that needs to take place throughout the process, both at top management and employee level. As well as the establishment of a good culture of transparency, people involvement and communication, including through non-financial awards.

All these have been used for proposing a corpus of good practices.

Regarding the contributions that my thesis has made, and not yet studied by the literature, is the importance of a specific management structure for emerging risks, within banks according to each key stage of risk management.

Indeed, although emerging risk management frameworks are gradually proposed by institutions and organisations, they are not specifically aimed at banks. However, this sector is increasingly regulated and faces a multitude of risks that have a significant impact on our global economy. Also, until now institutions and organisations have proposed risk management structures by types of emerging risks, but again this was not sufficient due to the interdependence between these risks.

My research also uncovered differences between the types of banks: commercial banks versus investment banks versus clearing banks versus financial regulator banks. In addition, another comparison was made between small versus large structures. This has never been presented, especially as emerging risks they face, as well as their internal resources and the process of managing emerging risks depend largely on the size of the structures and their degree of regulation.

Moreover, we often read in the literature that the traditional risk management process is no longer sufficient to deal with emerging risks. However, my thesis shows that these risks can be included in the traditional risk categories, and that they can be analysed on two criteria: the probability of occurrence and their potential impact, like familiar risks.

Finally, my thesis also proposes a risk management timeline, never proposed before. I show that the reporting of these risks must be much more regular than for familiar risks and that mapping and scenario analysis exercises must also be regularly repeated after each event.

Further discussion

The aim of this thesis was to understand the process of considering emerging risks in the banking sector without a clearly defined time period.

Nevertheless, it would be interesting to study the impact of the covid crisis on the way emerging risks are taken into account by banks, and to compare it with the period before the crisis.

Furthermore, we have mainly studied the way emerging risks are considered by banks from an organisational point of view, for two reasons. The first is that the different exercises carried out at each phase of risk consideration, and especially the scenario quantification and stress-testing exercises, are so precise and regulated that they could be the subject of a thesis. Secondly, many organisations such as the *IRGC*, *PwC*, or academics such as Locklear, have already proposed tools

for their more technical management. Nevertheless, it might be interesting to make a comparison between the different reports on technical tools for managing these emerging risks for the banking sector.

Limits faced

During the writing of my thesis, I faced many limitations, both in the literature review part and in the empirical research part.

Indeed, as far as the literature research is concerned, I was careful to look at articles dating from before the financial crisis of 2007-2008, since until that period only financial risks were mainly considered. Operational risks, which include some emerging risks, have been considered more after this period as well as the awareness of some emerging risks such as climate risks that impact the banking sector nowadays.

Moreover, the above good practice recommendations are intended to help the banking industry better address emerging risks. However, as emerging risks are of different types, these rules remain general and more specific rules according to the type of risk may allow to better identify, assess or mitigate the risk.

Finally, as the interviews were only conducted with banks in Belgium, I was not able to distinguish between the way risks are managed in Belgium and in other countries.

Bibliography

Aabo T., Fraser JRS., Simkins BT. (2005). The rise and evolution of the chief risk officer: Enterprise risk management at Hydro One. *The Bank of America journal of applied corporate finance*. 17(3). 62-75.

Aebi V., Sabato G. & Schmid M. (2012). Risk management, corporate governance, and bank performance in the financial crisis. *Journal of Banking & Finance*. 36 (12). 3213-3226. <https://doi.org/10.1016/j.jbankfin.2011.10.020>

Aksel K.H. (n.d.). *Organizing a financial institution to deliver enterprise-wide risk management*. Retrieved from PricewaterhouseCoopers website: https://www.pwc.com.tr/en/assets/about/svcs/abas/frm/operationalrisk/articles/pwc_enterprisewidrisk.pdf

Aldasoro I., Gambacorta L., Giudici P. & Leach Th. (2020a). *Operational and cyber risks in the financial sector*. Retrieved from BIS website: <https://www.bis.org/publ/work840.htm>

Aldasoro I., Gambacorta L., Giudici P. & Leach Th. (2020b). *The drivers of cyber risk*. Retrieved from BIS website: <https://www.bis.org/publ/work865.htm>

Al-Farsi. (2020). The influence of chief risk officer on the effectiveness of enterprise risk management: Evidence from Oman. *International Journal of Economics and Financial Issues*. 10(1). 87-95. <https://doi.org/10.32479/ijefi.8932>

Allan N., Cante N., Godfrey P. & Yin Y. (2012). A review of the use of complex systems applied to risk appetite and emerging risks in ERM practice: Recommendations for practical tools to help risk professionals tackle the problems of risk appetite and emerging risk. *British Actuarial Journal*. 18(1). 163-234. Doi:10.1017/S135732171200030X

Ashby S., Buck T., Nöth-Zahn S. & Peisl Th. (2018). Emerging IT risks: Insights from German banking. *Geneva Papers on Risk & Insurance*. 43(2). 180-207. DOI:10.1057/s41288-018-0081-8

Aven & Renn. (2010). Response to Professor Eugene Rosa's viewpoint to our paper. *Journal of risk research*. 13(3). DOI: 10.1080/13669870903484369

Aven T. (2012). The risk concept—historical and recent development trends. *Reliability Engineering & System Safety*. 99. 33-44. <https://doi.org/10.1016/j.ress.2011.11.006>

Aven T. (2013). On the meaning of a black swan in a risk concept. *Safety Sciences*. 57. 44-51. <https://doi.org/10.1016/j.ssci.2013.01.016>

Aven T. (2015). Implications of black swans to the foundations and practice of risk assessment and management. *Reliability Engineering & System Safety*. 134. 83-91. <https://doi.org/10.1016/j.ress.2014.10.004>

Aven T. & Flage R. (2015). Emerging risk – Conceptual definition and a relation to black swan type of events. *Reliability Engineering and System Safety*. 144. 61–67. <https://doi.org/10.1016/j.ress.2015.07.008>

Aven T. & Ylönen M. (2019). The strong power of standards in the safety and risk fields: A threat to proper developments of these fields?. *Reliability Engineering & System Safety*. 189. 279-286. <https://doi.org/10.1016/j.ress.2019.04.035>

AXA. (2020). *AXA future risks report 2020*. Retrieved from: <https://www.axa.com/fr/magazine/future-risks-report-2020>

Belfius. (n.d.). *Rapports*. Retrieved from: <https://www.belfius.be/about-us/fr/investisseurs/resultats-rapports/rapports>

BIS. (2021). *Basel Committee publishes analytical reports on climate-related financial risks*. Retrieved April 16, 2021 from a press release: <https://www.bis.org/press/p210414.htm>

Baudino P. & Svoronos J-P. (2021). *Stress-testing banks for climate change – a comparison of practices*. Retrieved from BIS website: <https://www.bis.org/fsi/publ/insights34.htm>

Blockley D. (2013). Analysing uncertainties: Towards comparing Bayesian and interval probabilities'. *Mechanical Systems and Signal Processing*. 37(1-2). 30-42. <https://doi.org/10.1016/j.ymssp.2012.05.007>

Bolton P., Després M., L. A. Pereira da Silva, Samama F. & Svartzman R. (2020). *The green swan: Central banking and financial stability in the age of climate change*. Retrieved from the BIS website: <https://www.bis.org/publ/othp31.pdf>

Buehler K., Carpineti M., Michel-Kerjan E., Nauck F. & Serino L. (2020). *A unique time for chief risk officers in insurance*. Retrieved from McKinsey&Company website <https://www.mckinsey.com/business-functions/risk/our-insights/a-unique-time-for-chief-risk-officers-in-insurance>

Cantle N. (2011). A review of the use of complex systems applied to risk appetite and emerging risks in ERM practice: Abstract of the London discussion. *British Actuarial Journal*. 18(1). 235-256. Doi:10.1017/S1357321713000135

Christiansen U., Thrane S. (2014). The prose of action: The micro dynamics of reporting on emerging risks in operational risk management. *Scandinavian Journal of Management*. 30(4). 427-443. <https://doi.org/10.1016/j.scaman.2014.08.006>

Chapelle A. (2019). *Lessons from a decade of top 10 op risks*. Retrieved from Risk.net website: <https://www.risk.net/risk-management/6735386/lessons-from-a-decade-of-top-10-op-risks>

Chapelle A. (2020). *Gestion des risques opérationnels : Guide des meilleures pratiques en banque et assurance*. Montreuil: Pearson France.

Chief Risk Officer (CRO) Forum's Emerging Risk Initiative. (2006). CRObriefing: *Emerging risk initiative: Position paper: Climate Change & Tropical Cyclones in the North Atlantic, Caribbean and Gulf of Mexico*. Retrieved from: <https://www.thecroforum.org/wp-content/uploads/2012/10/CRObriefingEmergingRiskInitiative-2.pdf>

Conforti R., La Rosa M., Fortino G., ter Hofstede A.H.M., Recker J. & Adams M. (2013). Real-time risk monitoring in business processes: A sensor-based approach. *Journal of Systems and Software*. 86(11). 2939-2965. <https://doi.org/10.1016/j.jss.2013.07.024>

COREP Support. (n.d.). *What is COREP?*. Retrieved July 02, 2021 from: <http://www.corep.support/what-is-corep.html>

COSO. (2004). *Enterprise risk management — Integrated framework: Executive Summary*. Retrieved from: <https://www.coso.org/documents/coso-erm-executive-summary.pdf>

COSO. (2018). *Enterprise risk management: applying enterprise risk management to environmental, social and governance-related risks*. Retrieved from: <https://www.coso.org/Documents/COSO-WBCSD-ESGERM-Guidance-Full.pdf>

Council of the EU. (2018). *Money laundering: Council adopts conclusions on an action plan for enhanced monitoring*. Retrieved from a press release: <https://www.consilium.europa.eu/en/press/press-releases/2018/12/04/money-laundering-council-adopts-conclusions-on-an-action-plan-for-enhanced-monitoring/>

CRO Forum. (2019). *Emerging risk initiative: Major trends and emerging risk radar: May 2019 update*. Retrieved from: https://www.thecroforum.org/wp-content/uploads/2019/07/CRO-ERI_Emerging-Risk-RadarTrends_May-2019-Update.pdf

CRO Forum. (2020). *Emerging risk initiative: Major trends and emerging risk radar: 2020 update*. Retrieved from: <https://www.thecroforum.org/wp-content/uploads/2020/06/ERI-Risk-Radar-2020-update.pdf>

CRO Forum. (2021). *Emerging risks initiative: Major trends and emerging risk radar*. Retrieved from: <https://www.thecroforum.org/wp-content/uploads/2021/06/ERI-Risk-Radar-2021.pdf>

Deloitte (2018). *Cyber risk and regulation in Europe: A new paradigm for banks*. Retrieved from: https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu_deloitte-cyber-risk-regulation-europe.pdf

Deloitte. (2021). *Global risk management survey, 12th edition: A moving target: Refocusing risk and resiliency amidst continued uncertainty*. Retrieved from: https://www2.deloitte.com/global/en/insights/industry/financial-services/global-risk-management-survey-financial-services.html?id=gx:2em:3int:GRMS_12:5eng:6fsi:20210102

Dickinson G. (2001). Enterprise risk management: Its origins and conceptual foundation. *The Geneva Papers on Risk and Insurance*. 26(3). 360-366. <https://doi.org/10.1111/1468-0440.00121>

Elseware, ORX. (2021). *Exploring risk exposure methodologies*. Retrieved from ORX website: <https://managingrisktogether.orx.org/research/risk-exposure-methodologies>

Emerging risk management framework. (2020). *The RMA Journal*, 102(10), 63-71. Retrieved from <https://www-proquest-com.proxy.bib.ucl.ac.be:2443/trade-journals/emerging-risk-management-framework/docview/2438197493/se-2?accountid=12156>

Euroclear. (2021). *Introduction to the sustainability report 2020*. Retrieved from <https://www.euroclear.com/newsandinsights/en/Format/Whitepapers-Reports/introduction-sustainability-report-2020.html>

European Central Bank. (2016). *Financial stability vulnerabilities stemming from cyber risks within financial market infrastructures*. Retrieved from: https://www.ecb.europa.eu/pub/financial-stability/fsr/focus/2016/pdf/ecb~8d1f9dc751.fsrbox201605_04.pdf

European Central Bank. (2017). *What is SREP?*. Retrieved July 03, 2021 from: <https://www.bankingsupervision.europa.eu/about/ssmexplained/html/srep.en.html>

European Central Bank. (2019). *ECB Banking Supervision: Risk assessment for 2020*. Retrieved from:

<https://www.bankingsupervision.europa.eu/ecb/pub/ra/html/ssm.ra2020~a9164196cc.en.html#toc1>

European Centrale Bank. (2019). *Anti-money laundering and combating the financing of terrorism – recent initiatives and the role of the ECB*. Retrieved from: <https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp191115~4369baad76.en.html>

European Central Bank. (2021). *ECB Banking Supervision: Assessment of risks and vulnerabilities for 2021*. Retrieved July 26, 2021 from: <https://www.bankingsupervision.europa.eu/ecb/pub/ra/html/ssm.ra2021~edbbea1f8f.en.html>

European Central Bank. (n.d.). *Anti-money laundering*. Retrieved July 26, 2021 from: <https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp191115~4369baad76.en.html>

European Commission. (2016). *Identifying emerging risks for environmental policies*. Future Brief 13. Retrieved from: https://ec.europa.eu/environment/integration/research/newsalert/pdf/emerging_environmental_risks_early_warnings_FB12_en.pdf

European Commission. (2017). *Science for environment policy: 'Emerging risks' identified as first of four key stages in a risk cycle*. Retrieved from: https://ec.europa.eu/environment/integration/research/newsalert/pdf/emerging_risks_identified_as_first_of_four_key_stages_in_risk_cycle_495na4_en.pdf

Financial Reporting Council. (2011). *Boards and risk: A summary of discussions with companies, investors and advisers*. Retrieved from: <https://www.frc.org.uk/getattachment/b88db2b6-af08-4a0e-9755-ab92de1268c2/Boards-and-Risk-final-Sept-2011.pdf>

Financial Services Authority. (2009). *The Turner review: A regulatory response to the global banking crisis*: March 2009. Retrieved from: http://www.actuaries.org/CTTEES_TFRISKCRISIS/Documents/turner_review.pdf

Flage R., Aven T., Zio E. & Baraldi P. (2014). Concerns, challenges, and directions of development for the issue of representing uncertainty in risk assessment. *Risk Analysis*. 34(7). 1196-1207. <https://doi-org.proxy.bib.ucl.ac.be/2443/10.1111/risa.12247>

Florin M-V. (2013). IRGC's approach to emerging risks. *Journal of risk research*. 16(3-4). 315-322. <https://doi.org/10.1080/13669877.2012.729517>

Fraser, I. & Henry, W. (2007). Embedding risk management: structures and approaches. *Managerial Auditing Journal*. 22 (4). 392-409. Doi:10.1108/02686900710741955

Galand V. (2019). *Réglementation CRR II - CRD V : Une mise à jour attendue*. Retrieved from EY website: https://www.ey.com/en_lu/banking-capital-markets/reglementation-crr-ii---crd-v---une-mise-a-jour-attendue

GAFI. (n.d.). *Who we are*. Retrieved July 26, 2021 from: <https://www.fatf-gafi.org/about/>

Giovannoni E. Quarchioni S. & Riccaboni A. (2016). The role of roles in risk management change: The case of an Italian bank. *The European accounting review*. 25(1). 109-129. <https://doi.org/10.1080/09638180.2014.990475>

Goffin J. (2021). *La BCE ancre sa politique monétaire dans le XXIème siècle*. L'Echo: July 9, 2020: p.3

Gordon L., Loeb., Tseng CY. (2009). Enterprise risk management and firm performance: A contingency perspective. *J. Account. Public Policy*. 28. 301-327. Doi: 10.1016/j.jaccpubpol.2009.06.006

Grace M.F., Leverty J. T., Philips R.D. & Shimpi P. (2015). The value of investing in enterprise risk management. *The Journal of Risk and Insurance*. 82(2). 289-316. Retrieved from: <https://www.jstor.org/stable/26482965>

Gramlich D. & Walker Th. (2020). Emerging risks: Concluding remarks. In Walker Th., Gramlich D., Bitar M. & Fardnia P. (Eds). *Ecological, Societal, and Technological Risks and the Financial Sector*. (pp. 1-10). Switzerland: Palgrave Macmillan. Doi: <https://doi.org/10.1007/978-3-030-38858-4>

Hall M., Mikes A. & Millo Y. (2015). How do risk managers become influential? A field study of toolmaking in two financial institutions. *Management Accounting Research*. 26. 3-22. <https://doi.org/10.1016/j.mar.2014.12.001>

Hargrave M. (2020). *Investment bank*. Retrieved June, 21, 2021 from Investopedia website: <https://www.investopedia.com/terms/i/investmentbank.asp>

Härle Ph., Havas A., Kremer A., Rona D. & Samandari H. (2015). *The future of bank risk management*. Retrieved from McKinsey&Company website: <https://www.mckinsey.com/business-functions/risk/our-insights/the-future-of-bank-risk-management>

Haugen S. & Vinnem J.E. (2015). Perspectives on risk and the unforeseen. *Reliability Engineering and System Safety*. 137. 1-5. <https://doi.org/10.1016/j.ress.2014.12.009>

Hayne C. & Free C. (2014). Hybridized professional groups and institutional work: COSO and the rise of enterprise risk management. *Accounting, Organizations and Society*. 39(5). 309-330. <https://doi.org/10.1016/j.aos.2014.05.002>

Heakal R. (2020). *What is the Glass-Steagall act?* Retrieved June, 21, 2021 from Investopedia website: <https://www.investopedia.com/articles/03/071603.asp>

Holmquist E. (2019). Hiring a Chief Risk Officer. *The RMA Journal*. 102(1). 46-55. Retrieved from <https://www-proquest-com.proxy.bib.ucl.ac.be:2443/docview/2352150440?accountid=12156>

Iraci J.A. & Rogers C. (2018). A framework for emerging risks. *The RMA Journal*. 101(1). Retrieved from: https://rmajournal.org/rmajournal/september_2018/MobilePagedArticle.action?articleId=1417015#articleId1417015

IRGC. (2010). *The emergence of risks: Contributing factors*. Executive summary: IRGC. Retrieved from: https://irgc.org/wp-content/uploads/2018/09/Exec-Summary_IRGC_ContributingFactorsToRiskEmergence2010.pdf

IRGC. (2011). *Improving the management of emerging risks: Risks from new technologies, system interactions, and unforeseen or changing circumstances*. Report. Retrieved from: https://irgc.org/wp-content/uploads/2018/09/irgc_er2conceptnote_2011.pdf

IRGC. (2014). *Emerging risk governance*. Report: IRGC. Retrieved from: https://irgc.org/wp-content/uploads/2018/09/IRGC-EmergingRiskGovernance_6June2014.pdf

IRGC. (2015). *IRGC guidelines for emerging risk governance: Guidance for the governance of unfamiliar risks*. Report: IRGC. Retrieved from: <https://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/IRGC-Emerging-Risk-WEB-31Mar.pdf>

IRGC. (2017). *Governance of emerging risks: guidelines for the governance of unfamiliar risks*. Report: IRGC. Retrieved from: <https://irgc.org/risk-governance/emerging-risk/a-protocol-for-dealing-with-emerging-risks/>

Jain R., Nauck F., Poppensieker Th. & White O. (2020). *Meeting the future: Dynamic risk management for uncertain times*. Retrieved from McKinsey&Company website: <https://www.mckinsey.com/business-functions/risk/our-insights/meeting-the-future-dynamic-risk-management-for-uncertain-times>

Jonkman S. & Diagne M. (2016). A framework for monitoring emerging risks to banking systems & regulatory response. *International Journal of Government Auditing*. 43(3). 26-27. Retrieved from <https://www-proquest-com.proxy.bib.ucl.ac.be:2443/docview/1814345229?accountid=12156>

Jovanović A.S. & Löscher M. (2013). *iNTeg-Risk project: How much nearer are we to improved “early recognition, monitoring and integrated management of emerging, new technology related risks”?*. Project, iNTeg-risk (early recognition, monitoring and integrated management of emerging, new technology related risks). European Commission. Retrieved from: <https://cordis.europa.eu/docs/results/213345/final1-jovanovic-integrisk2013-v15aj06092013.pdf>

Kagan, J. (2021). *Commercial bank*. Retrieved June, 21, 2021 from Investopedia website: <https://www.investopedia.com/terms/c/commercialbank.asp>

Kaplan R.S. & Mikes A. (2012). *Managing risks: A new framework*. Retrieved from Harvard Business Review website: <https://hbr.org/2012/06/managing-risks-a-new-framework>

Kaplan R.S., Leonard H.B. & Mikes A. (2020). *The risks you can't foresee*. Retrieved from Harvard Business Review website: <https://hbr.org/2020/11/the-risks-you-cant-foresee>

Khier I. L., Trautwein K., Huber A. & Stamm J. (2017). *The EU General Data Protection Regulation (GDPR) in the banking industry: An impact analysis on banks and wealth managers with the focus on Switzerland*. Rapport: PricewaterhouseCoopers. Retrieved from PricewaterhouseCoopers website: https://www.pwc.ch/en/publications/2017/gdpr_banking_industry_report_en.pdf

Klinke A. & Renn O. (2012). Adaptive and integrative governance on risk and uncertainty. *Journal of Risk Research*. 15(3). 273-292. Doi: 10.1080/13669877.2011.636838

Kruizinga A. (2021). *The taxonomy's role in transforming risk management*. Retrieved from PricewaterhouseCoopers website: <https://www.pwc.nl/en/topics/blogs/reshaping-the-risk-taxonomy.html>

L'Echo. (2021). *Les signalements de fraudes à la FSMA ont augmenté de 50% en deux ans*. Retrieved from : <https://www.lecho.be/entreprises/services-financiers-assurances/les-signalements-de-fraudes-a-la-fsma-ont-augmente-de-50-en-deux-ans/10282134.html>

Liebenberg A.P. & Hoyt R.E. (2003). The determinants of enterprise risk management: Evidence from the appointment of Chief Risk Officers. *Risk Management and Insurance Review*. 6(1). 37-52. <https://doi.org/10.1111/1098-1616.00019>

Locklear K. (2011). *Emerging risk: An integrated framework for managing extreme events*. Retrieved from: https://web.actuaries.ie/sites/default/files/erm-resources/cp_extreme_integrated_framework_locklear.pdf

Lundqvist SA. (2014). An exploratory study of enterprise risk management: Pillars of ERM. *Journal of Accounting, Auditing & Finance*. 29(3). 393-429. Doi:10.1177/0148558X14535780

March J.G. & Shapira Z. (1987). Managerial perspectives on risk and risk taking. *Management Science*. 33(11). 1404-1418. Retrieved from: <https://www.jstor.org/stable/2631920>

May M. White O. & Wilson G. (2021). *A 2021 risk agenda for boards of directors at US banks*. Retrieved from McKinsey&Company website: <https://www.mckinsey.com/~media/mckinsey/industries/financial%20services/our%20insights/a%202021%20risk%20agenda%20for%20boards%20of%20directors%20at%20us%20banks/a-2021-risk-agenda-for-boards-of-directors-at-us-banks.pdf?shouldIndex=false>

Mazri Ch. (2017). (Re)Defining emerging risks. *Risk Analysis*. 37(11). 2053-2065. Doi: 10.1111/risa.12759

McKinsey&Company. (2015). *Willis Group on the changing risk landscape*. Retrieved from: <https://www.mckinsey.com/featured-insights/leadership/willis-group-on-the-changing-risk-landscape>

McKinsey&Company, ORX. (2018). *Transforming safely – the emerging practice of risk-managing change*. Retrieved from: https://managingrisktogether.orx.org/sites/default/files/public/orx-mckinsey_risk-managing_change_report.pdf

McKinsey&Company. (2020). *McKinsey on risk: New risk challenges and enduring themes for the return*. Retrieved from: <https://www.mckinsey.com/~media/McKinsey/Business%20Functions/Risk/Our%20Insights/McKinsey%20on%20Risk%20Issue%209%202020/McKinsey%20on%20Risk%20Number%209.pdf>

McKinsey&Company. (2021). *McKinsey on Risk: New risk challenges and enduring themes for the return*. Retrieved from <https://www.mckinsey.com/~media/McKinsey/Business%20Functions/Risk/Our%20Insights/McKinsey%20on%20Risk%20Number%2010%20Winter%202021/McKinsey-on-Risk-Number-10.pdf>

McShane MK., Nair A. & Rustambekov E. (2011). Does Enterprise Risk Management Increase Firm Value?. *Journal of Accounting, Auditing and Finance*. 26(4). 641-658. Doi: 10.1177/0148558X11409160

Meyer K, Mikes A. & Kaplan R.S. (2021). *When Every Employee Is a Risk Manager*. Retrieved from Harvard Business Review website: <https://hbr.org/2021/01/when-every-employee-is-a-risk-manager>

Mikes, A. (2008). *Risk management at crunch time: Are Chief Risk Officers compliance champions or business partners?*. Retrieved from: SSRN website: <https://ssrn.com/abstract=1138615>

Mikes A. (2009). Risk management and calculative cultures. *Management Accounting Research*. 20(1). 18-40. Doi: <https://doi.org/10.1016/j.mar.2008.10.005>

Moody's Analytics. (2011). *Common reporting framework (COREP) – FAQs*. Retrieved from: <https://www.moodyanalytics.com/-/media/faq/2011/2011-30-11-MA-COREP-FAQ.pdf>

National Bank of Belgium. (2021). *Rapport 2020 : Préambule-Développements économiques et financiers-Réglementation et contrôle prudentiels*. Rapport. National Bank of Belgium: Brussels

Nöth-Zahn S. (2017). *Enterprise Risk Management: Insights on emerging risks from the German banking sector* (Doctoral thesis). Edinburgh Napier University, Edinburgh

ORX. (2019). *ICAAP methodology study*. Summary report. Retrieved from: <https://engage.orx.org/download/icaap-methodology-study>

ORX. (2020). *Operational risk horizon 2020*. Retrieved from: <https://managingrisktogether.orx.org/sites/default/files/public/downloads/2020/09/orxoperationalriskhorizonsummaryreport2020.pdf>

ORX (2021). *Operational risk horizon 2021*. Retrieved from: <https://managingrisktogether.orx.org/operational-risk-research/operational-risk-horizon-2021>

Osborne Ch. (2020). *Covid-19 blamed for 238% surge in cyberattacks against banks*. Retrieved from ZCNet website: <https://www.zdnet.com/article/covid-19-blamed-for-238-surge-in-cyberattacks-against-banks/>

Pagach D. & Warr. R. (2011). The characteristics of firms that hire Chief Risk Officers. *The Journal of Risk and Insurance*. 78(1). 185-211. Doi:10.1111 /j.1539-6975.2010.01378.x

Polasky S., Carpenter S.R., Folke C. & Keeler B. (2011). Decision-making under great uncertainty: Environmental management in an era of global change. *Trends in Ecology & Evolution*. 26(8). 398-404. <https://doi.org/10.1016/j.tree.2011.04.007>

PricewaterhouseCoopers. (2009). *Extending Enterprise Risk Management (ERM) to address emerging risks: Exploring emerging risks*. Retrieved from: Online.

PricewaterhouseCoopers. (2015). *Risk in review: Decoding uncertainty, delivering value*. Retrieved from: <https://www.pwc.com/gx/en/audit-services/publications/assets/pwc-risk-in-review-2015.pdf>

Renn O., Klinke A. & van Asselt M. (2011). Coping with complexity, uncertainty and ambiguity in risk governance: A synthesis. *Ambio*. 40(2). 231-246. Doi: 10.1007/s13280-010-0134-0

Sarrazin H. & Willmott P. (2016). *Adapting your board to the digital age*. Retrieved from McKinsey&Company website: <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/adapting-your-board-to-the-digital-age>

Stauffer I. (2021). *Identification and management of new risks – key gaps and recommendations*. Retrieved from S&P Global website: <https://www.spglobal.com/esg/csa/yearbook/articles/identification-and-management-of-new-risks-key-gaps-recommendations>

Stupp C. (2019). *Fraudsters used AI to mimic CEO's voice in unusual cybercrime case*. Retrieved from: <https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402>

Talbi T. (2020). *Les cyberattaques contre les banques ont triplé pendant le confinement*. Retrieved from Les Echos website: <https://www.lesechos.fr/finance-marches/banque-assurances/les-cyberattaques-contre-les-banques-ont-triple-pendant-le-confinement-1223765>

Taleb N.N. & Rimoldy Ch. (2011). *Le cygne noir : La puissance de l'imprévisible*. Paris: Les Belles Lettres

The Banks.eu. (2020). *Banks in Belgium*. Retrieved June 9, 2021 from: <https://thebanks.eu/articles/banks-in-Belgium>

The Institute of Internal Auditors. (2004). *The role of internal auditing in enterprise-wide risk management*. London: The Institute of Internal Auditors. Retrieved from: <https://www.iiajapan.com/pdf/data/erm/ERM.pdf>

The World Bank. (n.d.). *Environmental and Social Policies*. Retrieved from: <https://www.worldbank.org/en/projects-operations/environmental-and-social-policies>

Tranchard S. (2018). *The new ISO 31000 keeps risk management simple*. Retrieved from ISO website: <https://www.iso.org/news/ref2263.html>

Walker Th., Gramlich D., Vico K. & Dumont-Bergeron A. (2020). Emerging risks: An overview. In Walker Th., Gramlich D., Bitar M. & Fardnia P. (Eds). *Ecological, Societal, and Technological Risks and the Financial Sector*. (pp. 1-10). Switzerland: Palgrave Macmillan. Doi: <https://doi.org/10.1007/978-3-030-38858-4>

Wetekamp J. (2021). *Three reasons to add a Chief Risk Officer to your C-Suite*. Retrieved from Ceoworld Magazine: <https://ceoworld.biz/2021/04/07/three-reasons-to-add-a-chief-risk-officer-to-your-c-suite/>

Weymann M. & Egloff R. (2018). *Identifying emerging risks: Early anticipation of the future risk landscape*. Retrieved from The Actuary website: <https://theactuarymagazine.org/identifying-emerging-risks/>

World Economic Forum. (2021). *The global risks report 2021: 16th edition: Insight report*. Retrieved from: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

Wszelaki J.W. (2016). Emerging risks in auditing and accountability. *The Journal of Government Financial Management*. 65(2). 26-31. Retrieved from: <https://www-proquest-com.proxy.bib.ucl.ac.be:2443/docview/1813624296?accountid=12156>

Zucker R. & Rowell D. (2021). *6 Strategies for Leading Through Uncertainty*. Retrieved from Harvard Business Review website: <https://hbr.org/2021/04/6-strategies-for-leading-through-uncertainty>

Appendices

Appendix 1: This table gives an overview of the distinction between an emerging risk and a familiar risk according to the literature and according to the interviews conducted

		Familiar risk	Emerging risk
Definitions		<i>“The effect of uncertainties on objectives”</i> (ISO, 2018)	<i>“Emerging risks are about unclear or changing framework conditions (...). Thus, while we may think of emerging risks as being primarily entirely new risks (...) some are known and familiar risks, but they become new or (re)emerging, as their contextual conditions change”</i> (Weymann & Egloff, 2018)
Examples		Internal data theft and fraud Credit risk	IT development New technologies (AI, nanotech.) Climate change New regulations
Main criteria	Knowledge of risk	Familiar risk	- New risk - Familiar risk
	Materialisation of risk	Already materialised	- Not yet materialised - Evolving on the external environment and over time
	Threatening or opportunity to be taken	Can be an opportunity or a threat	Can be an opportunity or a threat
	Regulations in place	Already regulated	New regulations are coming
	Identification	Easy to identify with past data	Difficult to identify in general
	Quantification	Quantification in terms of monetisation possible	Difficult to quantify in terms of probability of occurrence and in terms of monetisation
	Basis for assessment	Based on historical data	- Based on judgments - Lack of historical

			data
	Characteristics	- Uncertain effects - Low to high impact - Low to high degree probability of occurrence - Impact objectives and strategy	- High impact - Impact objectives and strategy - Different velocity - Uncertain nature and consequences - Increase in intensity and severity
Challenges		- Can lead to new risks	- Lack of regulations - Uncertainty regarding the consequences
Based on interviews realised	Approach used	- Backward-looking - Forward-looking	- Forward-looking
	Materialisation of the risk over time		Happened on a daily-basis or rarely
	Characteristics		Uncertainty regarding the impact
	Maturity of the risk management framework to deal with		Lack of maturity of the risk management framework to deal with this risk
	Monitoring	By quantitative KRIs	By qualitative KRIs

* The shaded part of the table contains characteristics given by the interviewed banks, not mentioned in the literature review.

Source: Tranchard S. (2018). The new ISO 31000 keeps risk management simple. Retrieved from ISO website: <https://www.iso.org/news/ref2263.html>

And Weymann M. & Egloff R. (2018). Identifying emerging risks: Early anticipation of the future risk landscape. Retrieved from The Actuary website: <https://theactuarymagazine.org/identifying-emerging-risks/>

Appendix 2: This table shows the different definitions of emerging risks that exist in the scientific literature

Definition of emerging risks	
Sources:	Definitions of emerging risks:
Allan, Cante, Godfrey & Yin (2012, p.177)	<i>“Emerging risks are the emergence of unintended consequences as a result of complex interactions between strategic objectives, existing risks, risk management interventions, business and regulatory environment, markets and people’s behaviour.”</i>
Aven & Vinnem (2007)	<i>“(…) the likelihood of loss, i.e. the probability of a certain consequence to occur in specific time and space under specified or insufficiently specified conditions.”</i>
Chief Risk Officer (CRO) Forum’s Emerging Risk Initiative (2006, p.11)	<i>“Emerging risks are risks which may develop or which already exist that are difficult to quantify and may have a high loss potential.”</i>
Choo (2005)	<i>“Emerging risks are risks that arise from erroneous information in the way information is collected and used and therefore do not allow for proper identification by banks.”</i>
European Commission (2016, p.5)	<i>“Emerging risks are, generally, those [risks] that have a high degree of uncertainty regarding the probability of occurrence and the amount of potential loss or harm.”</i>
International Actuarial Association (2008)	Emerging risks are “developing or already known risks which are subject to uncertainty and ambiguity and are therefore difficult to quantify using traditional risk assessment techniques”.
International Risk Governance Council (IRGC, 2010, p.5)	<i>“A new risk, or a familiar risk in a new or unfamiliar context (re-emerging). These risks</i>

	may also be rapidly changing (in nature). Although they may be perceived as potentially significant, at least by some stakeholders or decision-makers, their probabilities and consequences are not widely understood or appreciated.” “A risk that is new, or a familiar risk that becomes apparent in new or unfamiliar conditions.”
Locklear (2011, p.5)	“(…) a new (novel) manifestation of risk, of a type which has never before been experienced”
Weymann & Egloff (2018)	“Emerging risks are about unclear or changing framework conditions (...). Thus, while we may think of emerging risks as being primarily entirely new risks (...) some are known and familiar risks, but they become new or (re)emerging, as their contextual conditions change.”

Source: Allan N., Cante N., Godfrey P. & Yin Y. (2012). A review of the use of complex systems applied to risk appetite and emerging risks in ERM practice: Recommendations for practical tools to help risk professionals tackle the problems of risk appetite and emerging risk. *British Actuarial Journal*. 18(1). pp.179-1889. Doi:10.1017/S135732171200030X

Chief Risk Officer (CRO) Forum's Emerging Risk Initiative. (2006). CRObriefing: *Emerging risk initiative: Position paper: Climate Change & Tropical Cyclones in the North Atlantic, Caribbean and Gulf of Mexico*. Retrieved from: <https://www.thecroforum.org/wp-content/uploads/2012/10/CRObriefingEmergingRiskInitiative-2.pdf>

European Commission. (2016). *Identifying emerging risks for environmental policies*. Future Brief 13. Retrieved from: https://ec.europa.eu/environment/integration/research/newsalert/pdf/emerging_environmental_risks_early_warnings_FB12_en.pdf

IRGC. (2010). *The emergence of risks: Contributing factors*. Executive summary: IRGC. Retrieved from: https://irgc.org/wp-content/uploads/2018/09/Exec-Summary_IRGC_ContributingFactorsToRiskEmergence2010.pdf

Locklear K. (2011). *Emerging Risk: An Integrated Framework for Managing Extreme Events*. Retrieved from: https://web.actuaries.ie/sites/default/files/erm-resources/cp_extreme_integrated_framework_locklear.pdf

Weymann M. & Egloff R. (2018). Identifying Emerging Risks: Early anticipation of the future risk landscape. *The Actuary*. Retrieved from: <https://theactuarmagazine.org/identifying-emerging-risks/>

Appendix 3: The purpose of this table is to show the different characteristics and features of emerging risks according to Allan and al. (2012) which includes some of the features also cited by many other scholars

Characteristics
● Scale of impact ● Degree of impact ● Possibility of occurrence ● Dynamism ● Connectedness ● Speed of spreading ● Evolution
Common features of emerging risk
● Uncertainty: there is little information available and the frequency and severity is difficult to assess; ● Difficulty in quantification: risk is uncertain and the risk transfer may be questionable; ● No industry position: no single insurer wants to make the first move for fear of losing market share: cater for increased genetic testing by stipulating full disclosure clause; ● Difficulties for risk communication: there is the danger of <i>investors or management</i> reacting to phantom risks; ● Regulatory requirement: supervisory involvement is often necessary; ● Identification: while their existence is undisputed, they cannot necessarily be proven in a clear and comprehensive manner; ● Describability: it is possible to describe them, albeit not necessarily in a conclusive manner; ● Causality between risk source and resultant losses: in many cases, their technical/scientific causal relationship with respect to specific losses cannot be conclusively and verifiably proven and sound arguments supporting such a relationship can be established only conditionally; ● Assessability in monetary terms: the scope of their consequences can be assessed in monetary terms only inadequately and imprecisely.

* In order to differentiate between these two notions, the notion of characteristics refers, in this work, to what differentiates emerging risks from each other; whereas features are considered to be the qualifier of an emerging risk.

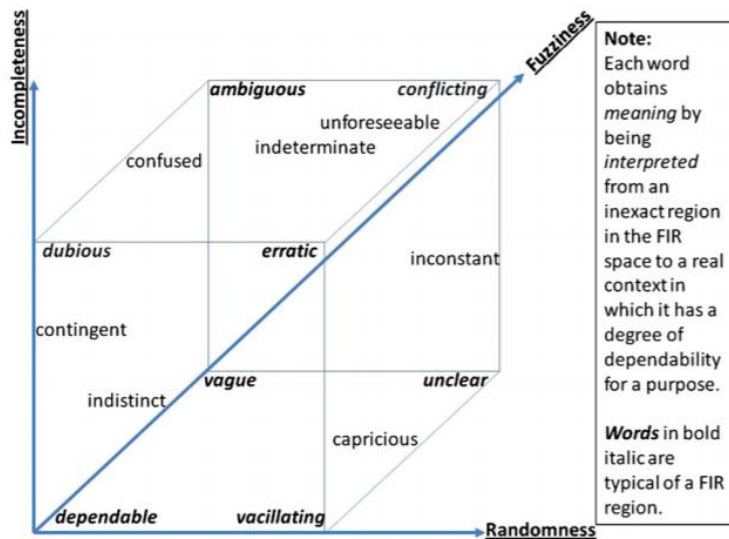
Source: Allan N., Cante N., Godfrey P. & Yin Y. (2012). A review of the use of complex systems applied to risk appetite and emerging risks in ERM practice: Recommendations for practical tools to help risk professionals tackle the problems of risk appetite and emerging risk. *British Actuarial Journal*. 18(1). pp.180-183. Doi:10.1017/S135732171200030X

Appendix 4: This table shows the three categories of emerging risks proposed by the *IRGC* (2017)

Risks with uncertain impacts	Risks in complex, interconnected systems	Risks resulting from changes in context
High uncertainty and a lack of knowledge about potential impacts and consequences (interactions with risk-absorbing systems). <i>e.g., applications of synthetic biology</i>	Increasing complexity, emerging interactions and systemic dependencies have the potential to lead to non-linear impacts and surprises. <i>e.g., systemic risks in energy or ICT systems</i>	Changes in context (social, regulatory, natural etc.) may alter the nature, probability and magnitude of expected impacts of previously known risks. <i>e.g., antimicrobial resistance</i>

Source: IRGC. (2017). *Governance of emerging risks: guidelines for the governance of unfamiliar risks*. Retrieved from: <https://irgc.org/risk-governance/emerging-risk/a-protocol-for-dealing-with-emerging-risks/>

Appendix 5: This graph will give you an overview of the characteristics of 'uncertainty' according to the three main axes which represent the three main characteristics whose interactions lead to other characteristics



* If we go deeper into the terms:

- Fuzziness means “*imprecision or vagueness of definition*”
- Incompleteness is what we do not know
- Randomness “*(...) is interpreted here as the lack of a specific pattern or purpose in some data (...)*”

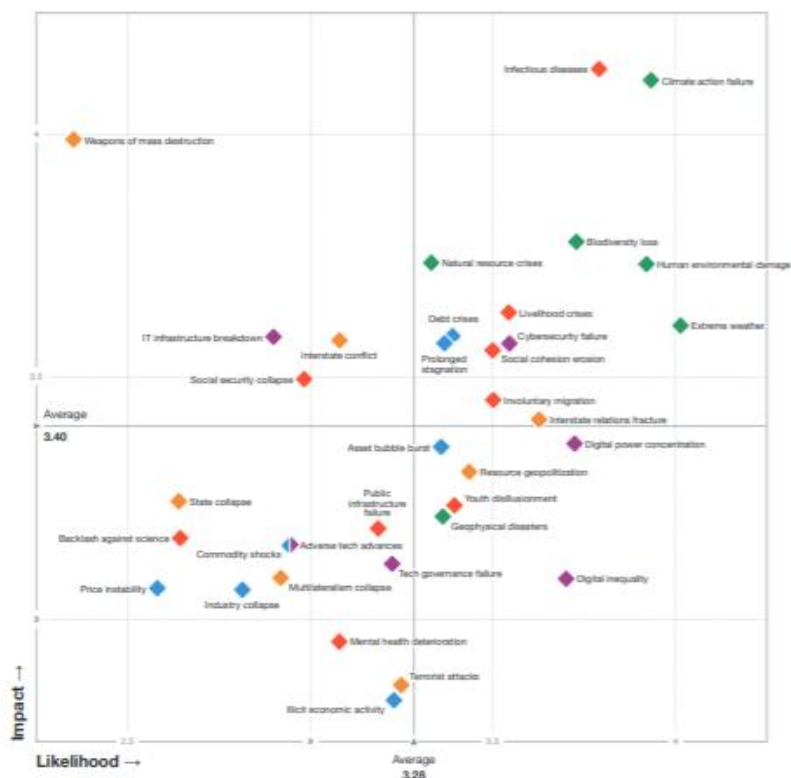
Source: Blockley D. (2013). Analysing uncertainties: Towards comparing Bayesian and interval probabilities'. *Mechanical Systems and Signal Processing*, 37(1-2), P.32.
<https://www.sciencedirect.com/science/article/abs/pii/S088832701200221X?via%3Dihub>

Appendix 6: This graph highlights the main emerging risks for the year 2021 according to the CRO Forum



Source: CRO Forum. (2021). *Emerging risks initiative: Major trends and emerging risk radar*. p.3. Retrieved from: <https://www.thecroforum.org/wp-content/uploads/2021/06/ERI-Risk-Radar-2021.pdf>

Appendix 7: This graph highlights the main emerging risks for the year 2021 according to the *World Economic Forum*



Source: World Economic Forum. (2021). *The global risks report 2021: 16th edition: Insight report*. p.12.
Retrieved from: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

Appendix 8: This table highlights the twelve factors that the *IRGC* (2010) believes cause emerging risks

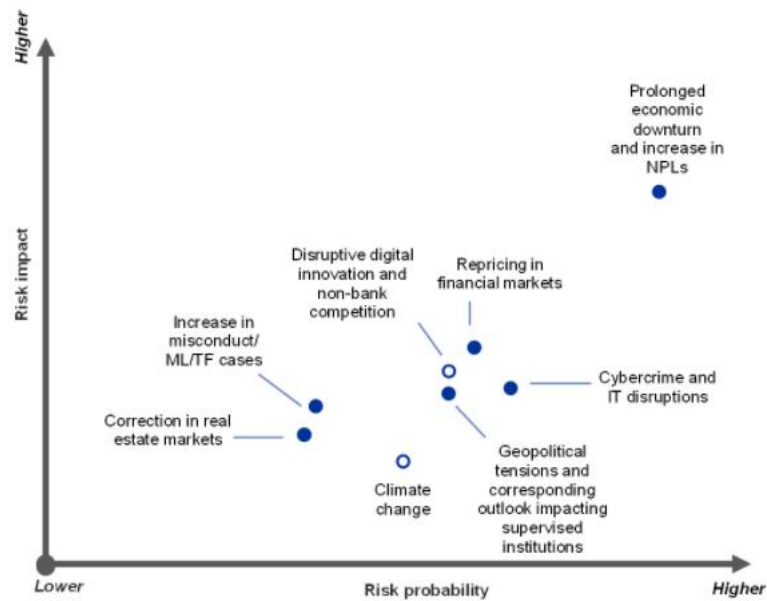
Factors	Explanations
Scientific unknowns	<i>“Dealing with emerging risks inevitably requires dealing with scientific unknowns. These unknowns, whether tractable or intractable, contribute to risks being unanticipated, unnoticed, and over- or underestimated.”</i>
Loss of safety margins	<i>“The level of connectivity in many of today’s social and technical systems is greater than in the past and the interconnections are increasing. The pace at which these systems operate is becoming faster and many are operating under higher levels of stress. This can lead to tight-coupling of components within systems and to loss of safety margins – a loss of slack or buffering capacity that leaves systems more vulnerable to disruption and thus increases the likelihood that new risks will emerge.”</i>
Positive feedback	<i>“Systems exhibiting positive feedback react by amplifying a change or perturbation that affects them. Positive feedback tends to be destabilising and can thus amplify the likelihood or consequences of an emerging risk.”</i>
Varying susceptibilities to risk	<i>“The consequences of an emerging risk may be different from one population to another. Geography, genetics, experience and wealth are just some of the possible contextual differences that create varying susceptibilities to risk.”</i>
Conflicts about interests, values and science	<i>“Public debates about emerging risks seldom</i>

	witness a clear separation between science, values, and interests. The conflicts that result have the potential to contribute to fertile ground for risk emergence or amplification. For example, emerging risks may be amplified when efforts to assess them and take early management measures encounter opposition on the grounds of contested science or incompatible values.”
Social dynamics	“Social change can lead to potential harm. In other circumstances, it can attenuate potential harm. It is therefore important for risk managers to identify, analyse and understand changing social dynamics.”
Technological advances	“Risk may emerge when technological change is not accompanied by appropriate prior scientific investigations or post-release surveillance of the resulting public health, economic, ecological and societal impacts. Risks are further exacerbated when economic, policy or regulatory frameworks (institutions, structures and processes) are insufficient, yet technological innovation may be unduly retarded if such frameworks are overly stringent.”
Temporal complications	“A risk may emerge or be amplified if its time course makes detection difficult (e.g., the adverse effects of the risk only become evident after a long period of time) or if the time course does not align with the time horizons of concern to analysts, managers and policymakers.”
Communication	“Risks may be complicated or amplified by untimely, incomplete, misleading or absent communication. Effective communication that

	<i>is open and frank can help to build trust. In many cases, such communication can attenuate, or lead to better anticipation and management of, emerging risks.”</i>
Information asymmetries	<i>“Information asymmetries occur when some stakeholders hold key information about a risk that is not available to others. These asymmetries may be created intentionally or accidentally. In some cases, the maintenance of asymmetries can reduce risk, but in others, it can be the source of risk or the amplification of risk by creating mistrust and fostering non-cooperative behaviours.”</i>
Perverse incentives	<i>“Perverse incentives are those that induce counterproductive or undesirable behaviours, which lead to negative, unintended consequences. Such incentives may lead to the emergence of risks, either by fostering overly risk-prone behaviours or by discouraging risk prevention efforts.”</i>
Malicious motives and acts	<i>“Malicious motives give rise to emerging risks and therefore practitioners need to consider intentional as well as unintentional causes of risk. Malicious motives and acts are not new, but in a globalised world with highly interconnected infrastructures (e.g., trade agreements and information and communication systems) they can have much broader-reaching effects than in the past.”</i>

Source: IRGC. (2010). *The Emergence of risks: Contributing factors. Executive summary*: IRGC. pp.6-7.
Retrieved from: https://irgc.org/wp-content/uploads/2018/09/Exec-Summary_IRGC_ContributingFactorsToRiskEmergence2010.pdf

Appendix 9: This graph highlights the key risk drivers for the year 2021 according to the *European Central Bank Banking Supervision*



Source: European Central Bank. (2021). *ECB Banking Supervision: Assessment of risks and vulnerabilities for 2021*. Retrieved July 26, 2021 from: <https://www.bankingsupervision.europa.eu/ecb/pub/ra/html/ssm.ra2021~edbbea1f8f.en.html>

Appendix 10: This table shows the main emerging trends for the year 2021, according to each risk category

Emerging trends that have an influence on emerging risks on the financial market				
	European Central Bank (2021)	CRO Forum (2021)	Deloitte survey (2021) ¹⁰	McKinsey (2021)
External of the banking sector				
Economical	- Prolonged economic downturn and increase in NPLs - Repricing in financial markets - Correction in real estate markets	- Monetary policies	- Global financial crisis - Credit quality deterioration	
Environmental	- Climate change	- Extreme weather - Climate change transition - Climate tipping points - Biodiversity		- Climate change
Geopolitical	- Geopolitical tensions and corresponding outlook impacting supervised institutions	- Geopolitical conflict - Political instability - Evolving terrorism - Protectionism		- Interconnectedness - Supply chain
Legal and regulatory	- Misconduct, money laundering and terrorist financing	- Legal and regulatory uncertainty		- Data privacy
Social		- Pandemics	- Global	- Changing customer

¹⁰ Based on a survey realised among 57 financial institutions worldwide, 16% of which have banking as their core business

			pandemics	expectations
Technological	- Cybercrime and IT disruptions - Disruptive digital innovation and non-bank competition	- Cyber risks - Critical infrastructure blackouts - Supply chain		- Digital disruption and data - IT and cyber risks
Internal of the banking sector				

Source: European Central Bank. (2021). *ECB Banking Supervision: Assessment of risks and vulnerabilities for 2021*. Retrieved July 26, 2021 from: <https://www.bankingsupervision.europa.eu/ecb/pub/ra/html/ssm.ra2021~edbbea1f8f.en.html>

CRO Forum. (2021). *Emerging risks initiative: Major trends and emerging risk radar*. Retrieved from: <https://www.thecroforum.org/wp-content/uploads/2021/06/ERI-Risk-Radar2021.pdf>

Deloitte. (2021). *Global risk management survey, 12th edition: A moving target: Refocusing risk and resiliency amidst continued uncertainty*. Retrieved from: https://www2.deloitte.com/global/en/insights/industry/financial-services/global-riskmanagement-survey-financial-services.html?id=gx:2em:3int:GRMS_12:5eng:6fsi:20210102

McKinsey&Company. (2021). *McKinsey on Risk: New risk challenges and enduring themes for the return*. Retrieved from: <https://www.mckinsey.com/~media/McKinsey/Business%20Functions/Risk/Our%20Insights/McKinsey%20on%20Risk%20Number%2010%20Winter%202021/McKinsey-on-Risk-Number-10.pdf>

Appendix 11: This table shows the different stages in the management of emerging risks according to the authors

Chapelle (2020)	United Nation Environment Program (UNEP) by the European Commission (2017)	IRGC (2015)	PWC (2009)
Risk Identification	<i>“Risk knowledge”</i>	<i>“Make sense of the present and explore the future”</i>	<i>“Identify emerging risks relevant for the organisation”</i>
Risk assessment	<i>“Risk monitoring and predicting”</i>	<i>“Develop scenarios based on narratives and models”</i>	<i>“Assess the risks’s significance”</i>
Risk mitigation	<i>“Disseminating information”</i>	<i>“Generate risk management options & formulate strategy”</i>	<i>“Determine risks response strategies, considering collaboration with external parties”</i>
Risk monitoring	<i>“Risk Response”</i>	<i>“Implement strategy”</i>	<i>“Routinely monitor emerging risks through effective use of indicators”</i>
		<i>“Review risk development and decisions”</i>	

Source: Chapelle A. (2020). *Gestion des risques opérationnels : Guide des meilleures pratiques en banque et assurance*. Montreuil : Pearson France.

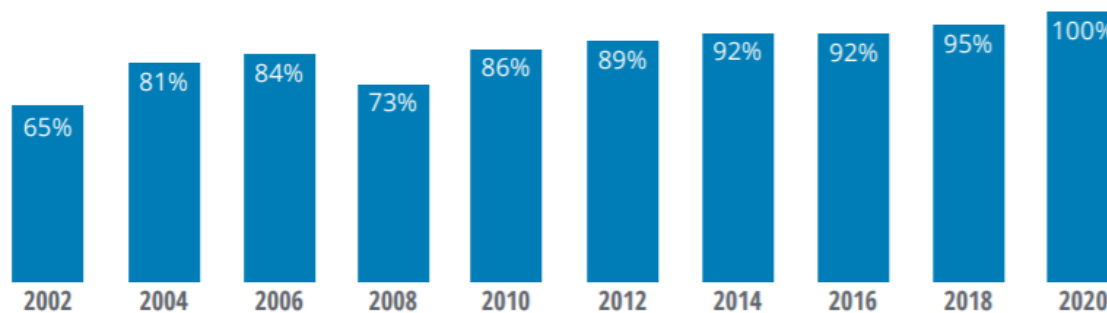
European Commission. (2017). *Science for environment policy : ‘Emerging risks’ identified as first of four key stages in a risk cycle*. Retrieved from: https://ec.europa.eu/environment/integration/research/newsalert/pdf/emerging_risks_identified_as_first_of_four_key_stages_in_risk_cycle_495na4_en.pdf

IRGC. (2015). *IRGC guidelines for emerging risk governance: Guidance for the governance of unfamiliar risks*. Report: IRGC. Retrieved from: <https://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/IRGC-Emerging-Risk-WEB-31Mar.pdf>

PricewaterhouseCoopers. (2009). *Extending Enterprise Risk Management (ERM) to address emerging risks: Exploring emerging risks*. Retrieved from: Online.

Appendix 12: This graph shows the presence of CROs, over the years, in 57 financial institutions interviewed by *Deloitte (2021)*, of which 16% have banking as their main activity

Organizations with a chief risk officer or equivalent position



Source: Deloitte Insights. (2021). *Global risk management survey, 12th edition: A moving target: Refocusing risk and resiliency amidst continued uncertainty*. Retrieved from: https://www2.deloitte.com/global/en/insights/industry/financial-services/global-risk-management-survey-financial-services.html?id=gx:2em:3int:GRMS_12:5eng:6fsi:20210102

Appendix 13: This table shows the cognitive biases and deficiencies faced by those involved in the management of emerging risks

Cognitive biases faced when making decisions about emerging risks:	
Names	Explanations
Anchoring	<i>“A bias where a person may jump to a conclusion based on the first piece of information he or she receives, or possibly hold on to a belief and jump to a conclusion.”</i>
Confirmation bias	<i>“Refers to the behavior where people seek information that confirms a preexisting belief, ignoring more objective information.”</i>
Egocentric interpretation of events	<i>“A condition in which individual perception is determined by the role one plays.”</i>
	<i>“Human tendency to overly discount the likelihood and impact of future events.”</i>
	<i>“Human preference for maintaining status quo, rather than having to deal with the challenges of implementing sometimes unpalatable preventive measures.”</i>
	<i>“Human reluctance to invest in preventative measures for problems which do not appear to be vivid and palpable, both personally and immediately relevant.”</i>
Illusion of understanding	<i>“[...]which is characterized by an unjustifiable belief that we understand what is going on is a world that is more complicated (or random) than [we] realize.”</i>
Organisational	<i>“Once a course of action has gathered support within a group, those not yet on board tend to suppress their objections—however valid—and fall in line”.</i>
Overconfidence	<i>“A result of people having too much faith in their own analyses or abilities—possibly leading, in the case of the financial industry,</i>

	<i>to higher-risk asset purchases or concentrated positions.”</i>
Planning fallacy	<i>“Occurs when a person underestimates the time needed to complete a task or overrates the ability to shape the future.”</i>
Positive illusions	<i>“Which give rise to an overly positive view of self, the world and the future.”</i>
Recency effect	Bias where only the latest events are taken into account
Representativeness	<i>“Occurs when we think recent events will continue into the future.”</i>
Retrospective distortion	<i>“Which is the ability to assess events with clarity only after the fact.”</i>

Source: Iraci J.A. & Rogers C. (2018). A framework for emerging risks. *The RMA Journal*. 101(1). Retrieved from: https://rmajournal.org/rmajournal/september_2018/MobilePagedArticle.action?articleId=1417015#articleId1417015

Locklear K. (2011). *Emerging risk: An integrated framework for managing extreme events*. Retrieved from: https://web.actuaries.ie/sites/default/files/erm-resources/cp_extreme_integrated_framework_locklear.pdf

Kaplan R.S. & Mikes A. (2012). *Managing risks: A new framework*. Retrieved from Harvard Business Review website: <https://hbr.org/2012/06/managing-risks-a-new-framework>

Appendix 14: This table shows the main emerging risks faced by the banks interviewed

Type of bank		Type of risks
Large commercial banks	Bank A	Business – Business model – Compliance – ESG Long interest rate & profitability – Outsourcing – Privacy and data
	Bank B	Climate – Cyber - Geopolitical – Regulatory
	Bank C	AML – Compliance – Credit – Cyber – IT – Operational and phishing attacks – Switch from financial → non-financial
	Bank D	Climate - Compliance – Credit – Data – Fraud - Market – information security and cyber– Phishing
Small commercial bank		Cyber-crime – Financial - Global warning – Interest rate – Pandemic– Strategic
Investment bank		ESG – Geopolitical - Health environment – Income – Regulatory - Sector
<i>Euroclear Bank</i>		AI and powerful analytics – ESG – Geopolitical – Inflation - New asset' classes and client' segments – Regulations – Rise of platforms - Security services – Service moderately and digitalisation foreign – Technological evolution
<i>World Bank</i>		Airplane crashes – Fraud – IT transformation

Type of risks	Type of banks				
	Large commercial banks	Small commercial bank	Investment bank	Securities clearing bank	Financial regulator bank
External					
Legal, regulatory and compliance risks	xxxx		x	x	
Environmental risks	xxx	x	x	x	
Technological risks	xxx	x		x	x
Geopolitical risks	xx		x	x	

Economical risks	xx	x	x	x	
Societal risks		x	x	x	x
Sectoral risks			x		
Internal					
Business and strategic risks	x	x	x	x	
Outsourcing risks	x				

* For this thesis, four large commercial banks, one small commercial bank, one investment bank, one securities clearing bank and one financial regulator bank were interviewed. The number of crosses in each box therefore represents the number of banks for which this risk is one of the main emerging risks they face.

It is also important to note that in some cases a cross represents several major risks. Indeed, in the case of Bank D (large commercial bank), it identified market and credit risks as two of the top three financial risks facing the bank. Nevertheless, these were summarized by a single cross in the economic risk box.

This is also the case for fraud risk, data risk and cyber risk, which are the top three non-financial risks faced by this Bank D and which were summarized by a single cross in the technology risk category.

For *World Bank* (financial regulator bank), the IT and fraud risks were highlighted as a cross in the category of technology risks.

The reason for grouping several risks into one category is that this table is primarily intended to give the reader an overview of the different categories of risks that banks face and not the numbers of each risk.

Appendix 15: This appendix outlines the reasons why ESG risks should be considered by banks and their strategies to address changing consumer choices

The consideration of ESG risks, which includes the aging population, climate transition and relocation of territory, is growing within banks. The reason is that banks have to respond to cultural changes in society and to the moral demands of consumers by ceasing to finance child labour, which is often reprimanded against large clothing or computer chains, but also with the implementation of rules prohibiting the financing of terrorism and anti-money laundering, which have significant reputational consequences.

Henceforth, consumer preferences are turning towards investments in the 'Green New Deal', whose historic term refers to the policy conducted by the U.S. President Roosevelt in 1933 to revive the U.S. economy following the Great Depression and the stock market crash of 1929. And to allow for a massive revival in employment through inflation.

The 'Green New Deal', term taken up in the United States and in Europe by political parties to talk about reviving the economy after the crisis of 2008 or the crisis of the covid or to fight against global warming with the 'European Green Deal' whose commitment was taken by the various European authorities in December 2019.

Moreover, with the arrival of competing banks such as *New B* which advocates a more sustainable and greener policy both in terms of investments and services and products offered, each bank is trying to respond to this new trend.

In order to understand this phenomenon of banks taking ESG risks into consideration, I visited the websites of the banks I interviewed, and it was clear that neither the small commercial bank nor the investment bank and Bank D were highlighting a greener and more sustainable strategy.

Nevertheless, Bank A clearly indicates its policy of taking these risks into account on its website by associating them with the 'United Nations Sustainable Goals' and by showing its affiliation with the *Belgian Alliance for Climate Action*. And indicates, in its annual report, that it has begun to develop an ESG risk framework, although it is not yet available.

The same bank has sought to reinvent itself to meet the new, more sustainable and greener market demands and to be more competitive by recently launching its investment platform, which offers a ranking of stocks according to the theme of the bank's sustainability policy, whether it be renewable energy, gender equality, etc.

As for Bank C, which had also highlighted climate risks as the main emerging risks it faces, it also underlines on its website its willingness to address more responsible investments as *Euroclear Bank* also said, although this is less visible than Bank A.

However, as a large financial group, it adds the importance of the influence it has in promoting equity, which is in line with Bank A's vision that the bank must be inclusive and inspiring for society. Probably because banks realise that they are not always seen in a positive manner, as the small commercial bank points out, for which the banks' business model is in danger and must be reviewed.

In comparison, *World Bank* also clearly states, on its website, its policy of respect for the environment and the protection of people and employees, as regularly stated by the CORO, and which he considers to be one of the reasons why the consideration of emerging risks is important, in addition to create value for clients.

Moreover, the organisation also indicates that it has taken environmental and social measures that must be respected by clients before any project can be financed by *World Bank*.

Although the organisation has not identified ESG risks as the main emerging risks, there is no doubt in my mind that these also need to be taken into account and properly managed. Indeed, the organisation targets poor countries, such as India and Africa, which are regularly affected by climate change that can dry up the land and undermine the economy of communities, or which do not have easy access to vaccines against covid and for which the organisation helps with distribution.

Moreover, geopolitical risks are also an emerging risk faced by the populations the *World Bank* is trying to help. The lack of respect for democratic principles and the refusal to establish the rule of law, although not mentioned in the interview, also has in my opinion many negative effects for these populations, such as a great disparity of means preventing access to water, education, and healthcare for large parts of communities and for which the organisation provides assistance.

In addition to environmental risks, ESG risks also include societal risks such as pandemic risks. I will refer here to the covid crisis. I was surprised that none of the banks mentioned pandemic risks as a major emerging risk and that only the investment bank stressed that it was surprised in the sense that the extent of the impact was somewhat overlooked.

In contrast, the *WEF* listed infectious disease risks as the fourth most likely emerging risk for the year 2021. Nevertheless, and although not indicated in the interview, Bank B has identified pandemics and infectious diseases as the top emerging risk on its online emerging risk report for

the year 2020, followed by climate change, cyber-attacks and geopolitical risks as indicated in the interview.

The reason why banks have not highlighted this is the fact that, like the retail and IT sectors, they have been impacted to a lesser extent, their activities being mainly digitalised and remotely accessible and thanks to the state aid provided to their clients.

Furthermore, according to an investment banker I met as part of an in-depth finance programme, he described the covid crisis as a period of growth for the global economy.

This period of growth is often a phase of the cycle where many mergers and acquisitions take place, as was the case in the banking sector with the acquisition of E*TRADE by the investment bank Morgan Stanley in October 2020, during the covid crisis. This may seem surprising in view of the announcement of a possible financial crisis at that time.

Appendix 16: This table shows the risks and steps in the risk management process for which banks ask for the help of external consultancy firms

	Type of banks				
	Large commercial Banks	Small commercial bank	Investment bank	Securities clearing bank	Financial regulator bank
Type of risks					
Legal, regulatory and compliance risks	xx	x		x	
Credit risks	xx				
Technological risks	x	x			
Outsourcing risks	x				
Environmental risks				x	
Societal risks				x	

	Type of banks				
	Large commercial banks	Small commercial bank	Investment bank	Securities clearing bank	Financial regulator bank
The process stage					
Benchmarking	x				x
Sharing inputs	xx	x	x		
Identification	x	x		Usually	
Assessment	xxxx		x	Maybe later on	
Mitigation	x				
Monitoring					

* For this thesis, four large commercial banks, one small commercial bank, one investment bank, one securities clearing bank and one financial regulator bank were interviewed. The number of crosses in each box therefore represents the number of banks for which this risk or this step is the reason for which banks ask for the help of external consultants.

World Bank (financial regulator bank) did not specify the risks or the stage of the process for which its audit team can sometimes call on external consultants.

Regarding *Euroclear Bank*, it says that it may use external consultants for ESG risk stress-testing exercises in the future because it currently has a sufficiently qualified team to manage the risks. Moreover, the bank also adds that in general it is for the identification of risks that it calls on consultants, after which the bank tries to be self-sufficient for the other stages of taking into account emerging risks.

Appendix 17: The table below shows the reasons, at each stage of risk management, why banks use consultants

Stages	Reasons
Identification	The top management prefers to rely on an opinion other than the one of its team and asks the consultancy firm to carry out an analysis of the possible risks it may face.
Assessment	Once banks have identified the risks themselves, they can use external consultants to gain access to more market or peer information to review with what they have done so far.
Mitigation	This stage requires experience and maintaining teams in this stage for a longer period of time than the bank may have. Often at this stage a legal consultant will be involved as partner contracts.
Monitoring	In general, external consultants are very rarely involved at this stage. But the bank may decide to outsource its monitoring process to a third party in order to reduce its costs and improve the quality of its monitoring.

* Given the divergent opinions on the stage at which banks use external consultants and on the suggestion of one of the banks interviewed, I had the opportunity to interview a consultant in risk management for financial institutions.

He told me that the biggest difficulty for banks is the management of risks that are not yet mature and therefore they cannot be sure that their management process is sufficiently effective until these events fully materialise. The necessary qualities are therefore agility in the process it develops and accepting that risk is not easily predictable.

Appendix 18: In this table, you will find a list of internal and external sources used by banks to collect information regarding emerging risks

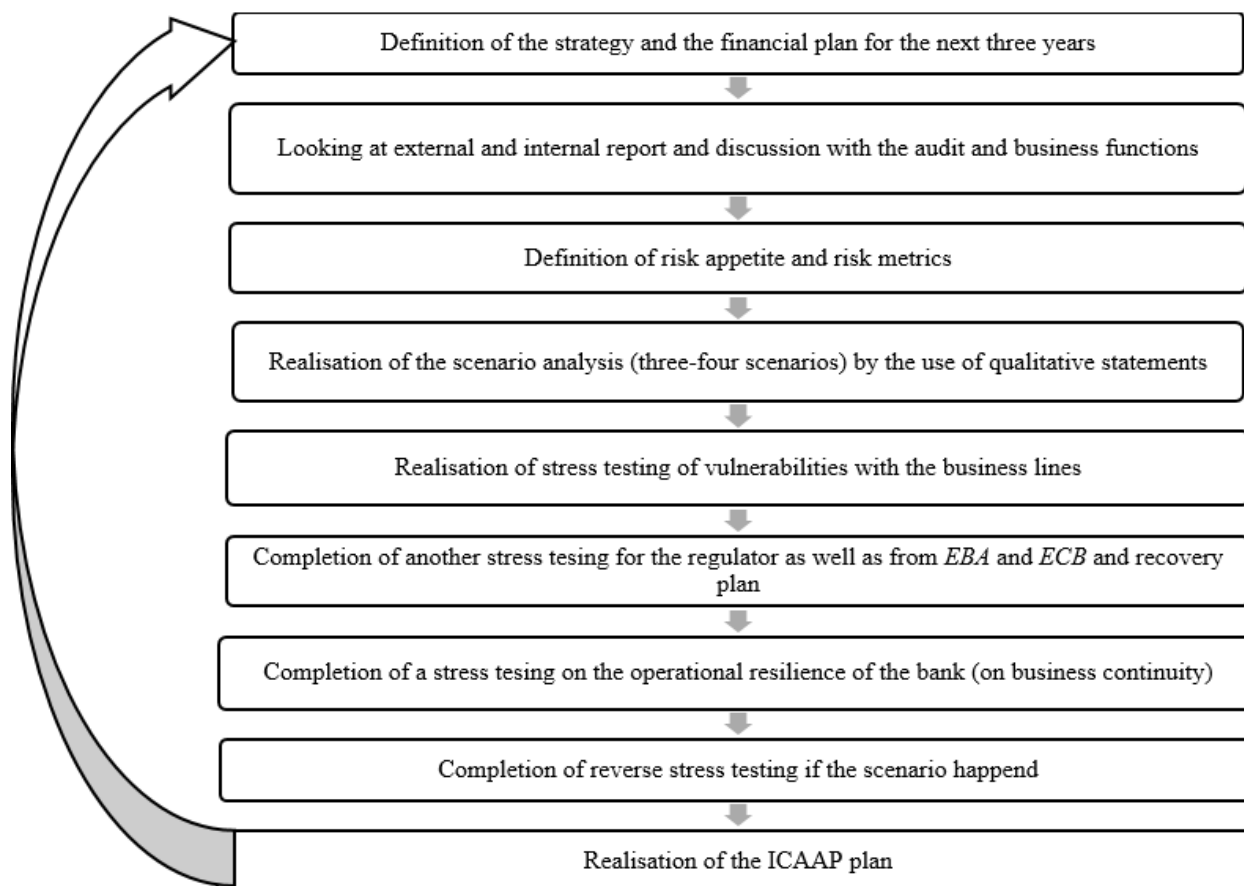
		Type of banks				
		Large commercial banks	Small commercial bank	Investment bank	Securities clearing bank	Financial regulator bank
Sources used to collect information						
Internal sources		- Internal report from each domain - Discussion with each department and with a Chief Economist - Survey regarding the top five risks for each domain - Identify if the strategy of the bank involves		- Internal discussion		

		new risks				
External sources	Report	- <i>World Economic Forum</i> report - <i>National Bank of Belgium</i> report - <i>European Centrale Bank</i> risks map - <i>International Monetary Fund</i> report - Consulting firms reports	- Group work from the <i>FEBELFIN (Fédération Belges des Entreprises Financière)</i> federation		- Consulting firms reports	- Regulatory reports and other general reports - <i>World Economic Forum</i> report - Consulting firms reports
	Other	- Daily newspapers or newspapers specialised in finance - Academic papers - External database: ORX	- ORX database - Meeting with banking associations - Open discussion with other bank' representative	- Industry' meetings organise by consulting firms	- Newspapers - Meeting with an external Chief Economist from another bank - Public database: ORX	- Newspapers - External Consultants - Academic papers - Discussion with other institution such as European

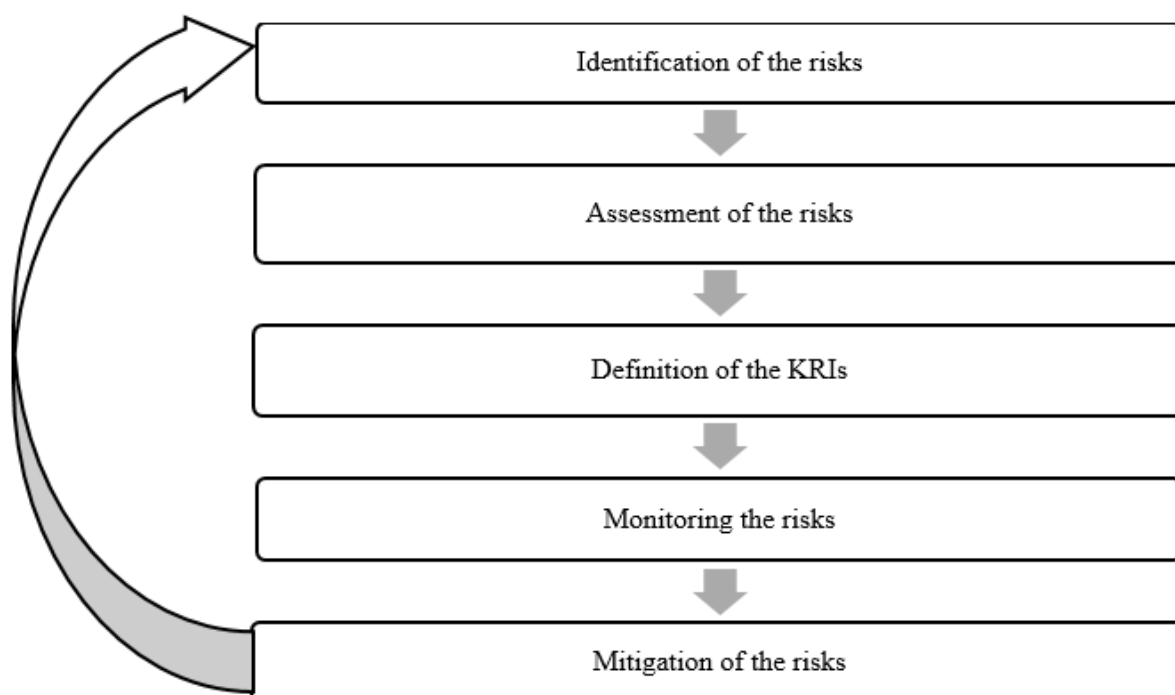
		or from the governance - Industry' meetings organise by consulting firms - Informal talk with CROs from other banks	s		- Industry' meetings	Investment Bank, universities
--	--	---	---	--	-------------------------	-------------------------------------

Appendix 19: The process built by Bank A to consider risks

1. The process to consider *familiar* risks in Bank A.



2. The process to consider *emerging* risks in Bank A



* When considering emerging risks, Bank A adopts a bottom-up approach where each year there is a discussion with the audit department and the front office, to identify all the risks the bank is facing. Which may be new risks due to the bank's strategy or due to the external environment in which the bank operates, and their action plan to mitigate them.

If the bank considers that the degree of risk is more important, it can propose an additional or more important action plan.

The top-down approach, also performed annually, is based on the risks identified in the institutional and supervisory reports and is mainly performed by the strategic risk management team.

One of the exercises carried out through this approach is to identify the top ten risks faced by the bank, ensure that they are well taken into account in the risk taxonomy, and in the risk mapping, after the definition of the bank's strategy and the drafting of its financial plan followed by the definition of the bank's risk appetite, and the limits.

The risk appetite, decided by the BofD and declined in each segment of the company and for each risks, is realised in different colors, and can be a percentage of income by non-performing loans.

But in case the income increases, the risk taken also increases to stay at the same level as decided by the BofD.

At the end of the year, the bank then performs stress testing exercises on potential vulnerabilities and establishes three to four scenarios addressing the liquidity, capital and profitability of it.

A second stress testing exercise, this time requested by the regulator, is also carried out, including the ICAAP exercise to ensure that the bank has enough capital to face possible events leading to economic losses, with a recovery plan.

Finally, a third stress testing exercise is performed, this time requested by the *EBA* and the *ECB*, in order to ensure that all banks can face the same economic shock and also to ensure the operational resilience of the bank with a fourth test of resilience where the bank tests its business continuity in case of IT services shutdown, for example.

This approach is an ongoing process for which there is no strict schedule, except when the regulator requires the exercise to be done and the financial plan to be written at the end of the year.

Nevertheless, the bank adds that for new risks, such as ESG risks, it follows a stricter planning, where risks are first identified, then evaluated and monitored via KRIs. However, in case indicators do not allow a good evaluation of emerging risks, the bank says it uses qualitative statements. Finally, these are integrated into the bank's framework.

Appendix 20: The process to consider emerging risks in Bank B

**A graph can hardly be proposed here, as some steps of the risk management process are missing and the bank does not disclose its entirely.*

In the case of the (large commercial) Bank B, it carries out a broad scan each year, following which it tries to identify the five main risks that can impact the company.

According to the bank, it is difficult to manage emerging risks like the familiar risks, and adds that it tends to treat them separately, which was the subject of a warning by the *ECB*.

Concerning the risk assessment phase and more particularly the scenario analysis phase, like the investment bank, it proposes two versions, one simpler where these are then deduced in potential macroeconomic drivers and another more advanced one, used for the management of emerging risks.

As for the actions taken, these vary according to the type of risk. In fact, cyber risks and climate risks have been in the bank's scan for a long time. And as far as climate risks are concerned, they have already been mitigated because, according to the bank, if it is not done now, it will not be done in the next decade.

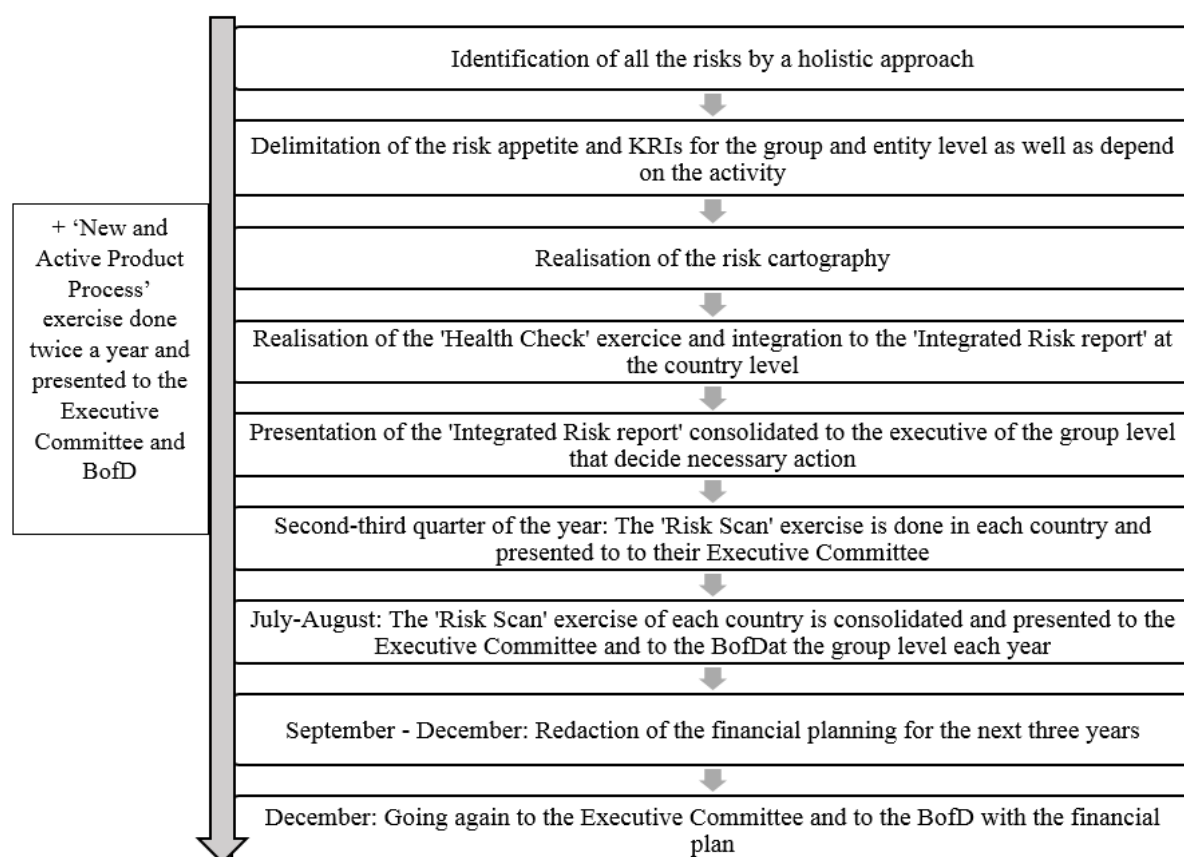
Nevertheless, action plan is done Mid-May, for the next three year as other banks. Regarding cyber risks, the timescale is different, these are discussed every month because they represent a daily challenge for the bank.

Regarding the quantification of scenarios, this is mainly a matter of judgement, as *World Bank* also says, and is a clear process.

Concerning the control phase, the bank says it uses KRIs proposed in studies or published by competitors.

Finally, regarding the reporting to the risk committee first and then to the BofD, it depends from one risks to another but regarding cyber risks, it is at least semi-annually.

Appendix 21: The process to consider emerging risks in bank C



* In the case of large commercial bank C, it does not only look at emerging risks. Indeed, the bank does not distinguish between so-called emerging risks and so-called familiar risks and thus adopt a holistic approach.

Once the top ten risks have been identified, the bank maps them according to their degree of impact and their time horizon of up to five years.

The reason why the bank does not assign an axis to the probability of the event taking place is because some so-called emerging risks such as cyber risks occur on a daily basis. The bank has several processes in place to deal with risks, these are detailed in the table below.

The first is called 'the Risk Signal Process' where once the main risks are identified, they are reported in the 'Integrated Risk Report', presented to the BofD eight times a year.

But before, in order to draft this report, the CROs of each country where the bank is established meet every month and discuss the information that needs to be reported to the executive and/or

that needs to be taken into account at group level. This reporting is therefore done at the level of each entity but also at the group level.

Once the report has been produced at the group level, with information from the various entities taken into account, it is discussed with the group's senior general managers and CROs and then presented to the Executive Committee, which can decide on any necessary action.

Then, another risk process is the 'Risk Scan', done each year during the second-third quarter of the year to be ready before the start of the redaction of the financial plan, done between September and December. For this report, each country is responsible for identifying their top risks and notifying their Executive Committee of them.

Then the group consolidates the information and identifies the top ten risks for the whole group, taken external reporting also into account. Which is then presented to the Executive Committee and the BofD, and reported in July/early August and again in December, after the financial plan is drafted.

Then comes the risk assessment stage where risks are taken into account in the financial plan, carried out annually and for a period of three years. Risks are then calculated in terms of p&l, capital, liquidity and impact on the strategy. Each country has to say how the top ten risks, defined at group level, will be addressed and mitigated at their level.

In addition, another process carried out by the bank is called 'New and Active Product Process' (NAPP), this one is carried out on a continuous basis for which numerous discussions with each country and each department are realised twice a year, in order to identify potential risks on the products offered by the bank.

The implementation of controls is made, by using KRIs, to ensure that the risk appetite and limits, defined by the BofD and the Executive Committee, are respected (mainly implemented for financial risks).

These indicators are then taken into account in the 'Integrated Risk Report' and will be measured monthly or quarterly. These limits, as you can see in the graph below, are defined both at the group level where each local entity implements them and defined new ones, as well as by type of activity of the bank.

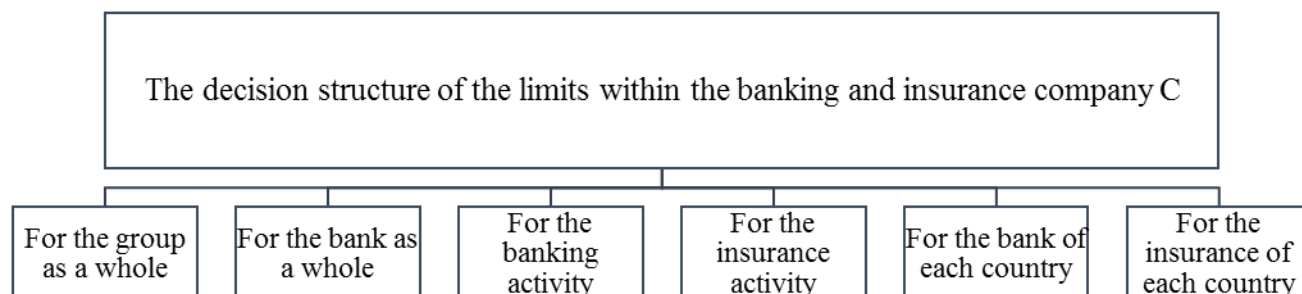
In addition to these different reports, there may be reports by type of risk, e.g. credit risks report, insurance report, etc., which will be discussed at the group level and by the team concerned by the risk.

However, the bank doesn't have to wait for these reports in case of major risks, in which case it can report the information directly to the Executive Committee and the to BofD.

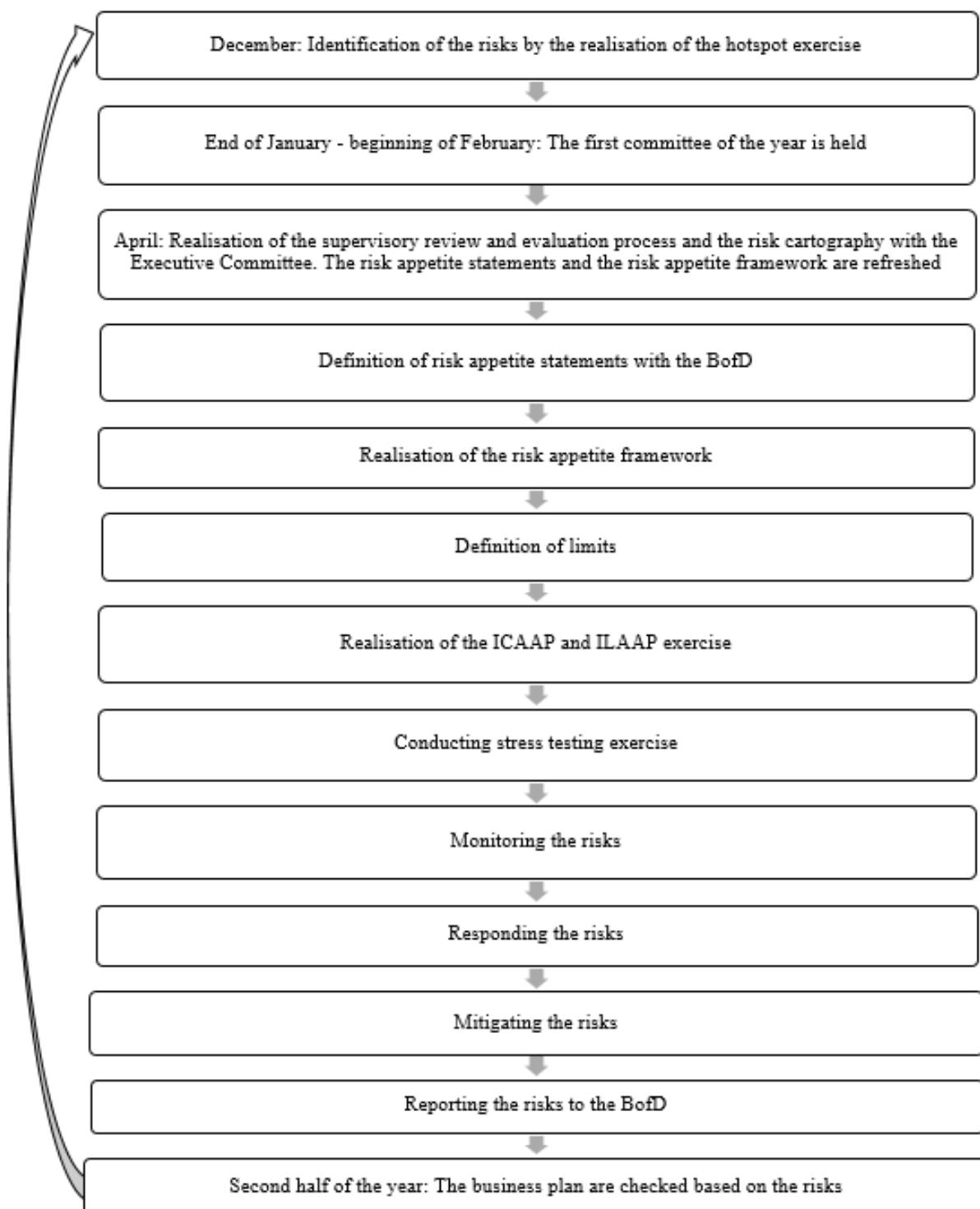
The different exercises done by Bank C realised at the group and/or the country level:		
Type of exercises	Levels involved	Explanations
Risk Signal exercise (Bottom-up approach)	Group level and country level	Fixed reporting: Done eight times per year and part of the 'Integrated Risk report', each CROs of each country explains the ten main risks they faced. ➔ Then they explain them to their Executive Committee ➔ Who reports to the group that consolidates the list of the top ten risks from each country ➔ The group discusses these risks with the different departments, also at the group level: Treasury, communication, legal, etc. ➔ A list of the top ten risks for the whole group is defined and presented to the Executive Committee and to the BofD of the group ➔ Action plans, based on the financial situation (capital, liquidity, p&l, etc) are decided, for the next three years, with the Executive Committee ➔ The information goes back to each countries that has to look at the list of the main risks for the whole group and the statements and to ensure that it is feasible at

		their country level.
Integrated Risk report (Bottom-up approach)	Group level and country level	Fixed reporting: Reported to the BofD eight times per year.
NAPP (New and Active Product Process) (Bottom-up approach)		Fixed reporting: Done twice a year by meetings with each countries and the different departments and reported to the Executive Committe and to the BofD.
If bank faced urgent risks	Group level	Adhoc reporting: The information is directly shared with the Executive Committee and BofD.

Levels at which limits are decided within the bank C



Appendix 22: The process to consider emerging risks in the bank D



* Now concerning the (large commercial) Bank D for which emerging risks are called 'hotspots risks', because more efforts are made to manage these risks and may be the subject of special meetings where the BofD asks for more in-depth information on them.

Regarding the risk assessment phase, the bank performs an annual update of its risk mapping with the Executive Committee which is then presented to the BofD.

This mapping is carried out according to an axis of maturity of the bank to take into account the potential emerging risks, and an axis of potential impact of risks.

Subsequently, the CRO of the bank convenes the various directors from the different departments to discuss the risks and mainly the risks whose action plans are not mature enough to mitigate them and which may negatively impact the bank's strategy by 2023.

In addition, the *ECB* also asked the bank to prepare an action plan in case a cyber risk paralyses its IT department. As well as in case a climate risk strongly impacts the bank's operations.

Once these risks have been mapped, they form part of the risk appetite framework that is reported to the BofD every quarter. In case of new risks, KRIs and limits are set.

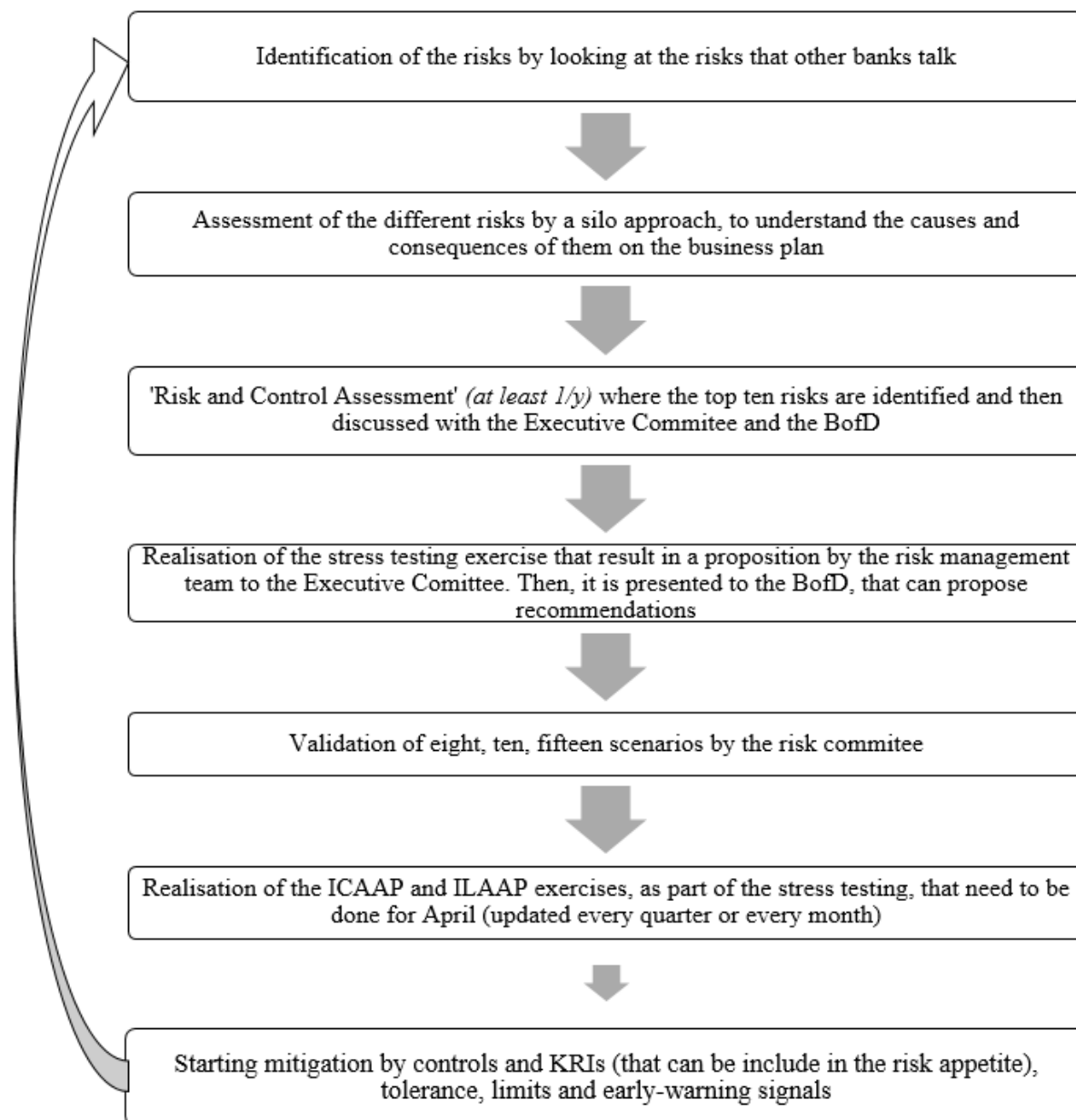
ICAAP and ILAAP exercises are then carried out by the second line of defence.

This process is realised in a cycle that is supported by the first line of defence. At the end of January-beginning of February, the first risk committee is held, which precedes the risk mapping that must be completed in April for presentation to the *ECB*.

Then, around June, the drafting of the business plan begins, which will be presented to the BofD in the second half of the year, and then the process starts again.

Finally, it is important to specify that the bank also has an insurance activity and that a distinction is made in the analysis of the scenarios depending on whether it concerns the banking or the insurance activity.

Appendix 23: The process to consider emerging risks in the small commercial bank



*The management of (emerging) risks, in the small commercial bank, starts with the 'Risk and Control Assessment'. In this exercise, the bank assesses the robustness of the company's internal controls based on past incidents or recommendations from external auditors and the regulator.

This exercise takes place at least once a year, in the form of a double four-hours workshop involving each department as well as the Compliance Officer, Data Protection Officer and various people from the risk department. It discusses the risks that occurred in the previous year and the

budget for the coming year to finally come up with a list of the top ten risks that the bank can deal with. They will then be discussed with the Executive Committee and the BofD.

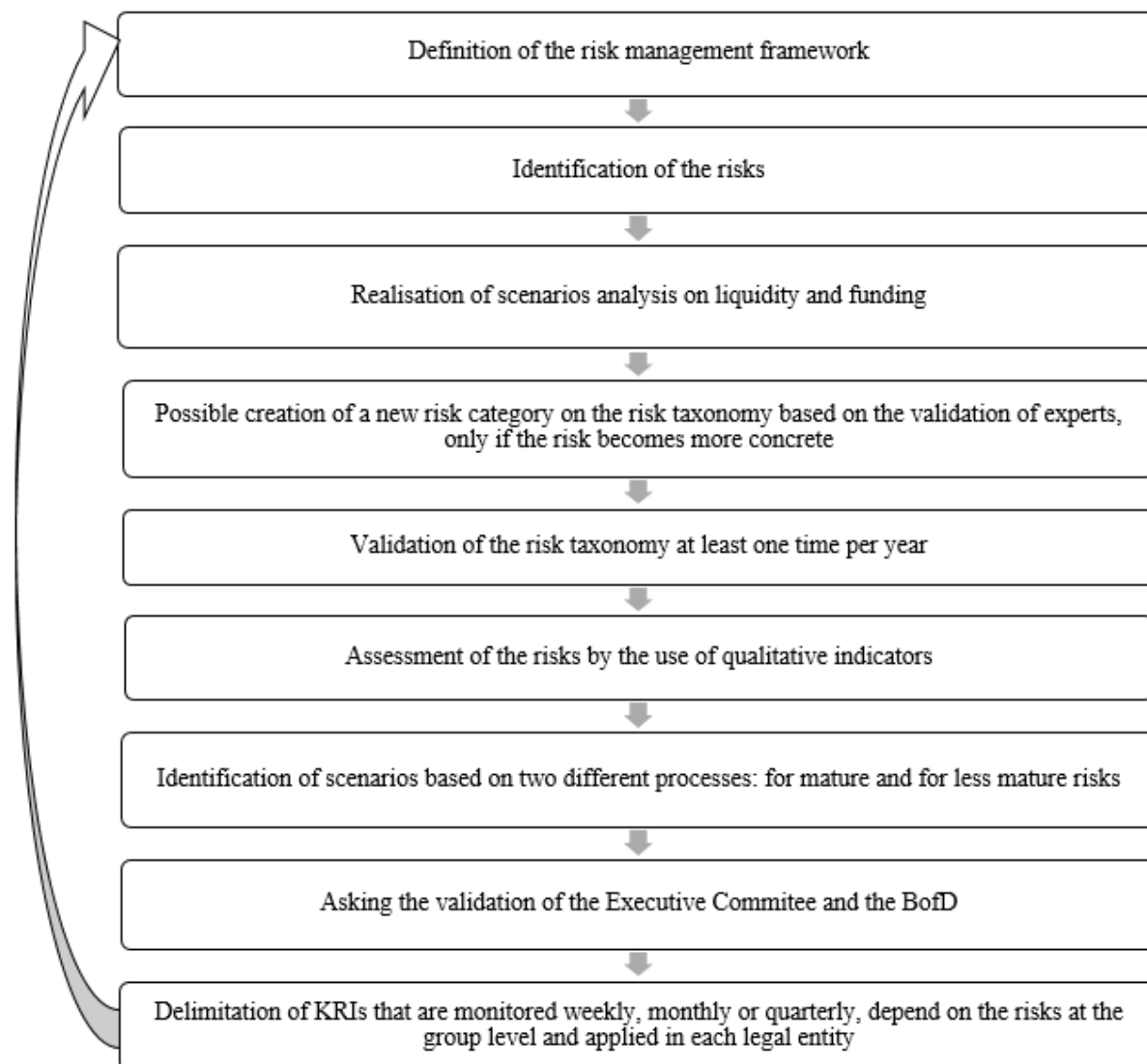
Then comes the stress testing phase where the bank will try to find out the impact of a risk on its strategy and financial situation. This exercise will then be presented to the Executive Committee which, if it agrees with it, will be presented to the BofD, which can propose recommendations.

The role of the risk committee is then to validate these scenarios which subsequently lead to the completion of the ICAAP and ILAAP exercises, which must be completed by April but reviewed on a monthly or quarterly basis and presented to the Executive Committee to ensure that the situation remains under control. This process is done on an ongoing basis.

Once the risk assessment is completed, the bank implements controls and KRIs. Depending on whether the risk is significant, the indicators will be declined into the risk appetite.

Finally, risk limits and risk tolerance will also be defined, as well as early warning signals in order to act at the first sign of a new risk which will then be reported to the BofD and a second level of KRI can be established at the level of the bank's activities.

Appendix 24: The process to consider emerging risks in the investment bank



*In the case of the investment bank, it has set up a risk management framework to structure the identification, assessment, and monitoring of risks.

The latter defines the risks faced by the bank, which are then communicated internally to those exposed to these risks, as well as to superiors.

Once all the risks have been identified, the bank carries out a scenario analysis, at least once a year, to assess the financial impact of these potential risks on the bank. In some cases, a new category of risk may be added to the existing taxonomy based on the advice of experts, at least once a month.

As a reminder, the investment bank considers emerging risks to be both, risks that have not yet materialised; or risks that are becoming more concrete and whose materialisation is becoming apparent. It is only in this second phase of emerging risks that they can be integrated into the risk management framework.

During the risk assessment phase, risks are assessed using qualitative indicators and once they have become more tangible, they can be quantified. The same thing was visible in Bank A for risks that are difficult to quantify, such as fraud risks.

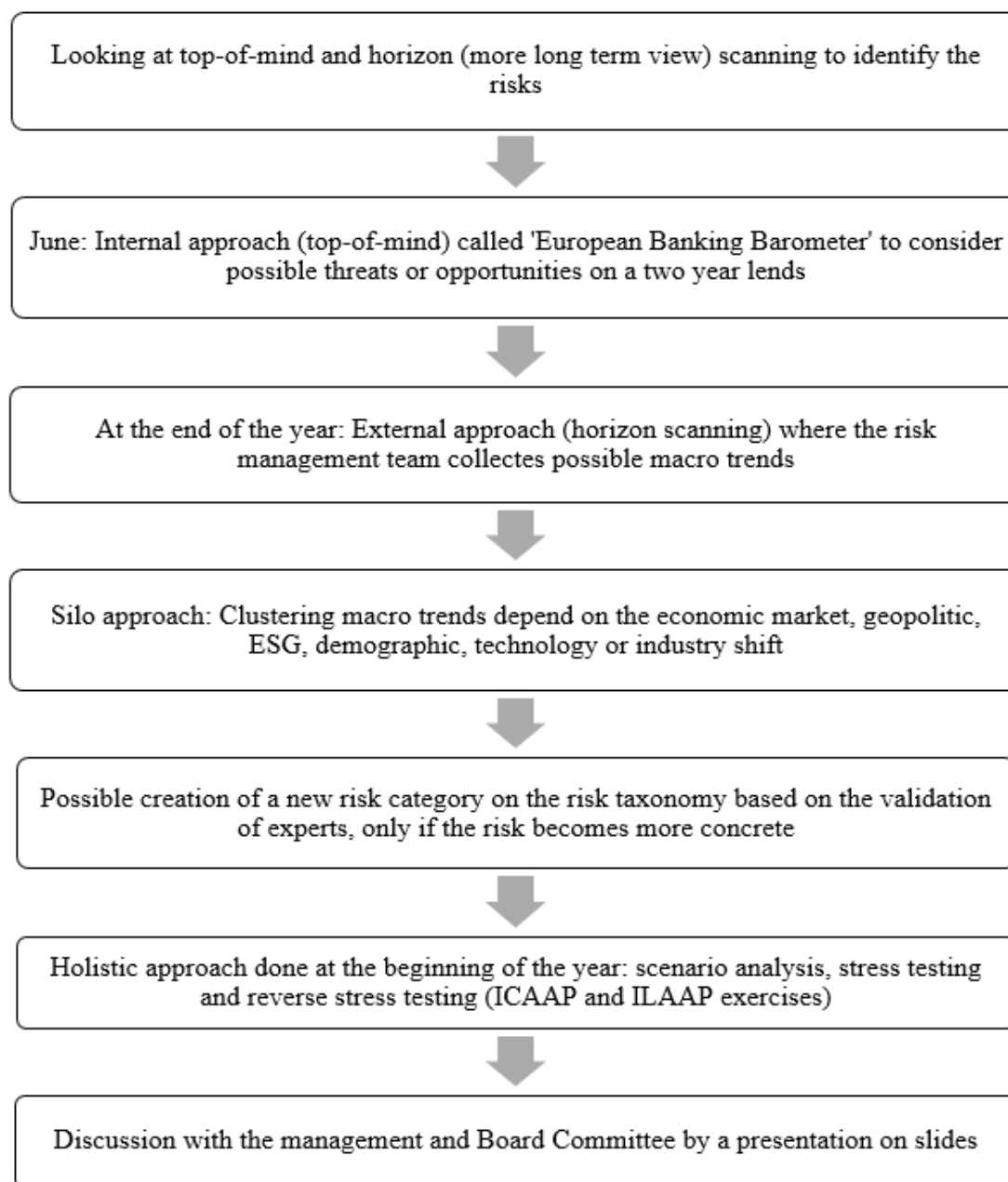
Then comes the step of quantifying the scenarios. For this, the bank calculates the possible impact of the financial and non-financial risks that the bank may face. Moreover, the bank distinguishes between mature and non-mature risks, as Bank A.

For the first category of risks, the bank takes into account past events and then extrapolates the financial impact and evaluates the potential future risks that will be modelled. In the case of non-mature risks, such as climate risks, the bank will analyse on the basis of defined parameters, potential decreases in value or revenues that may be generated by potential risks, based on research from academic or institutional sources.

Once these scenarios are completed, the information is shared with the Executive Committee and the BofD, who validate them.

Then, in order to control the risks, KRIs are defined, jointly with the business lines, both at the group level and then replicated within each legal entity and function line if needed. As some risks are cross-departments or depend on one department and one activity to another. And depending on the risks, they are monitored weekly, monthly or quarterly, which is mainly the case for emerging risks once they have been integrated into the framework.

Appendix 25: The process to consider emerging risks at *Euroclear Bank*



* Regarding *Euroclear Bank*, it identifies risks according to two different approaches depending on the duration.

The first one considers more the risks that it calls 'top-of-mind' and those that evolve over a longer horizon (horizon scanning). For the first approach, these are analysed using a tool it calls the 'European Banking Barometer' which consists of looking, once a year in June, at the main risks that the bank faces in its daily activities over the next two years.

The second approach, also carried out each year (towards the end of the year), is to look at the emerging events and trends taking place in the external environment. This latter exercise, carried out by the risk management team which is responsible for gathering information and aggregating it, requires more effort than the first as it requires preparatory work for workshops with the BofD and a more in-depth analysis than the first.

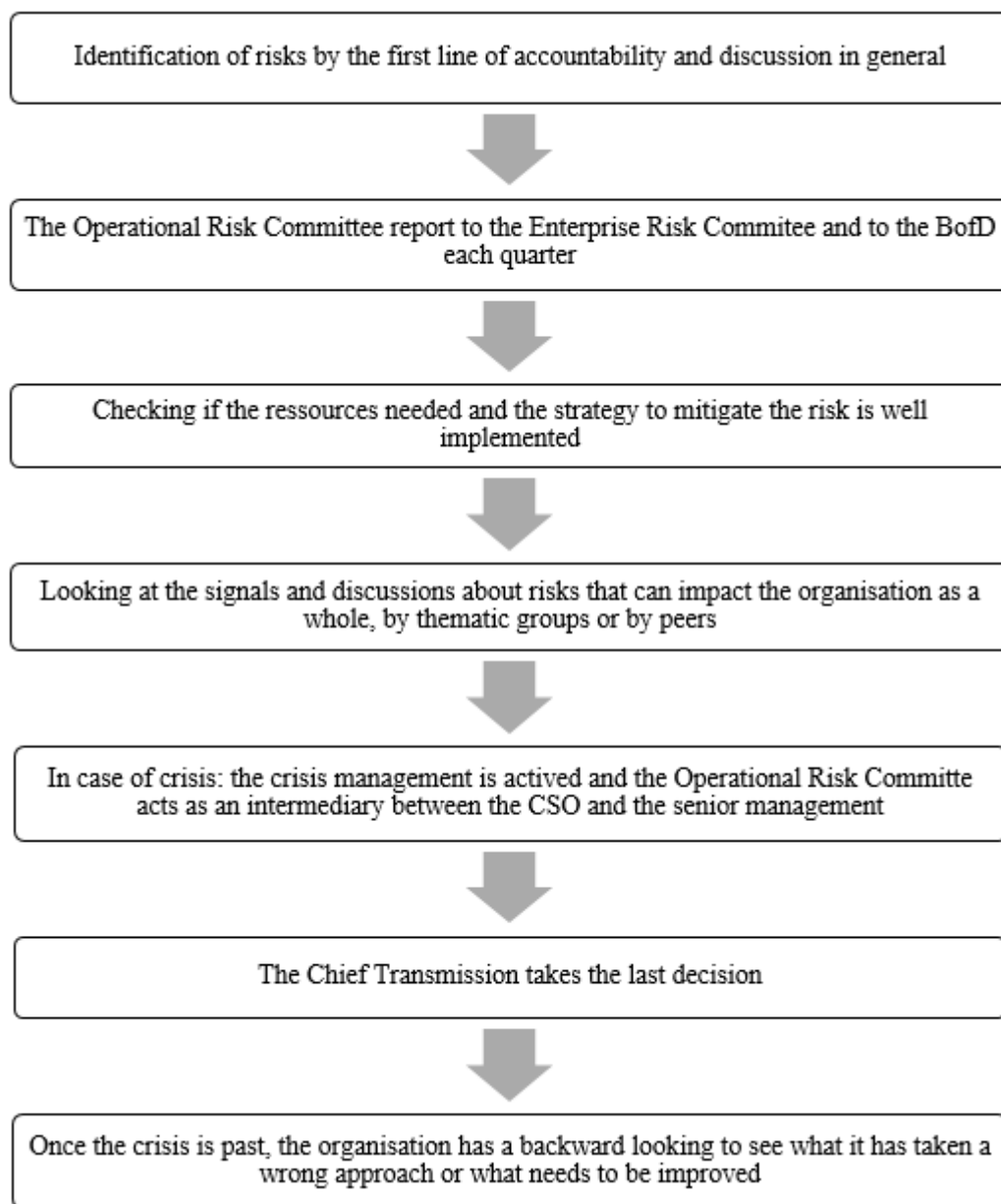
Once the information is collected, it is grouped by clusters: economic market, geopolitics, ESG, demographic, technology and the last one, industry shift, to then identify and assess the potential implications for the bank and the responses to be put in place.

The bank uses a silo approach where risks are looked at individually and then combined in the scenario analysis, stress testing and reverse stress testing exercises.

A dedicated meeting is then held for these exercises where information is shared via slides and where discussion is actively carried out with experienced Board members in order to compare ideas and feedback is given on the preparatory work carried out.

During the risk mapping phase, *Euroclear Bank* proposes four quadrants, as you can see in appendix 27, according to the degree of uncertainty of the risk and according to the possible impact on the bank, but only for the scanning horizon. In the ‘European Banking Barometer’ (EBB) exercise, risks are mapped according to the probability of the risk, which includes its uncertainty, and its severity.

Appendix 26: The process to consider emerging risks at *World Bank*



*Regarding *World Bank*, it is not subject to any regulations, and tries to establish its own rules based on the regulations in force. Nevertheless, throughout the process, the organisation is asking itself if it were regulated, like the other banks interviewed, how it should act.

The Operational Risk Committee has a quarterly discussion with the BofD, after discussions internally and with first line accountability about possible new risks or events that become more important over time such as cyber risks.

Then the organisation asks itself if its risk management level is sufficient and if all resources and risk mitigation strategies are in place. Secondly, a discussion among several people in the

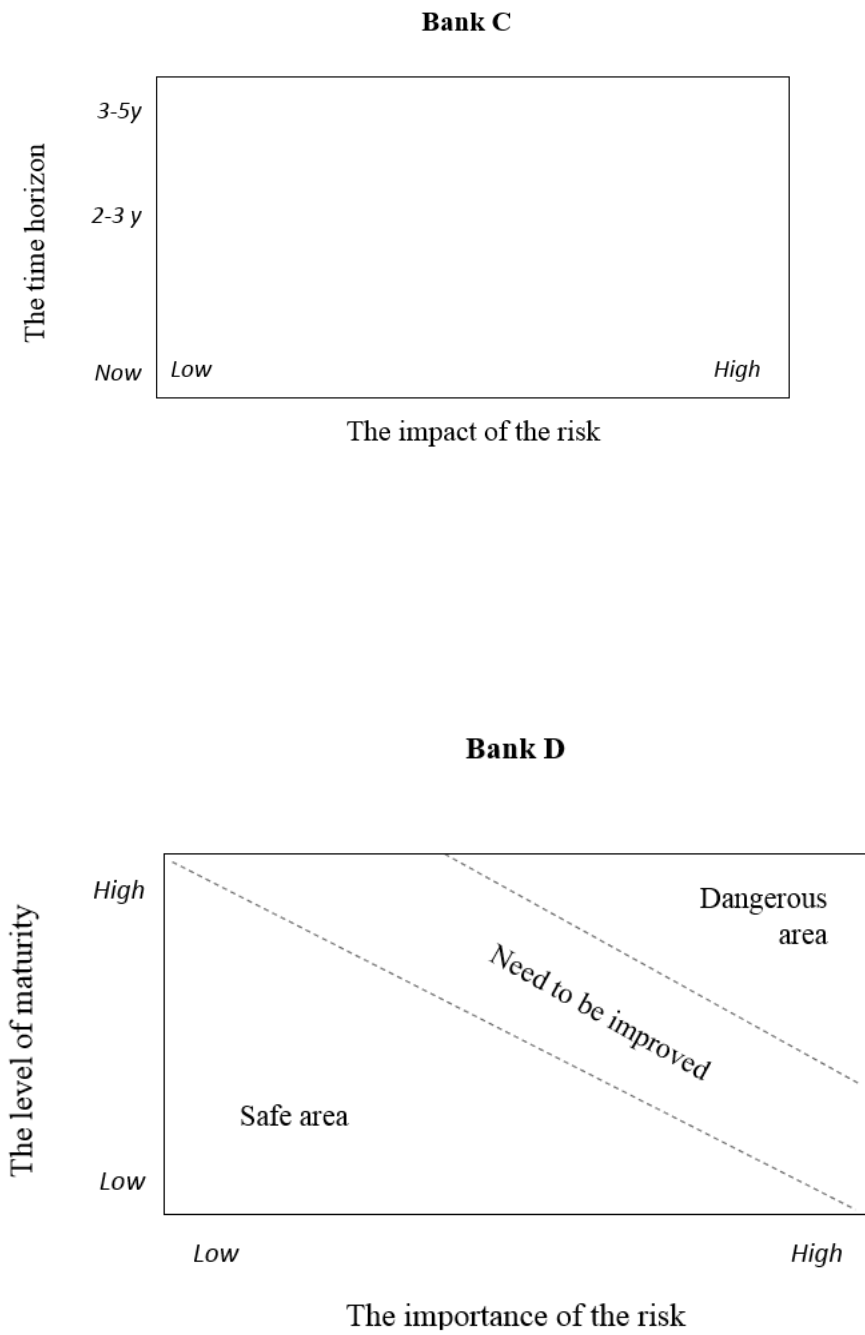
Operational Risk Committee, as well as between thematic groups and peers within the organisation is conducted. The reason for involving several people is to reduce possible biases and where the organisation discusses either a particular risk or several risks that may impact different business functions or the organisation as a whole.

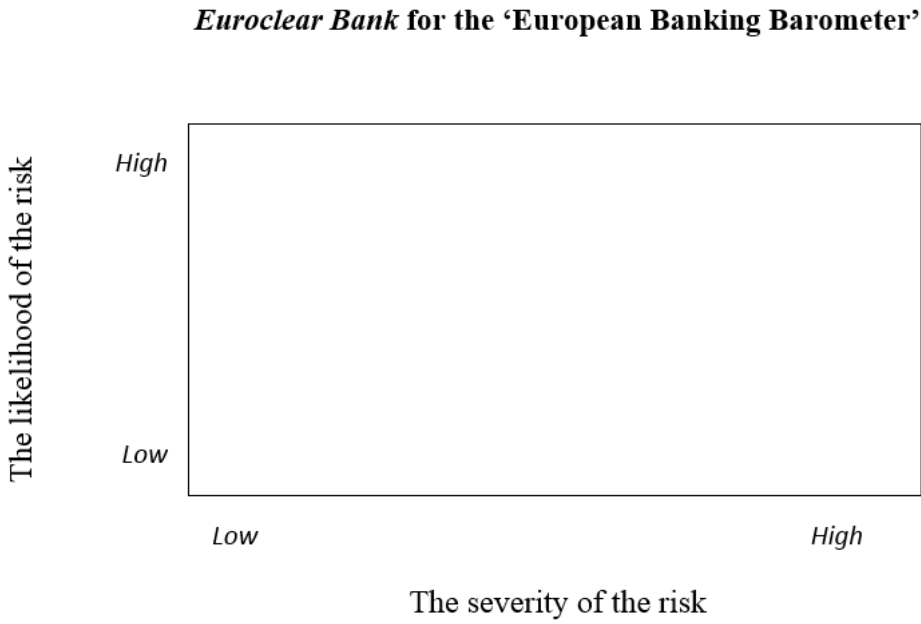
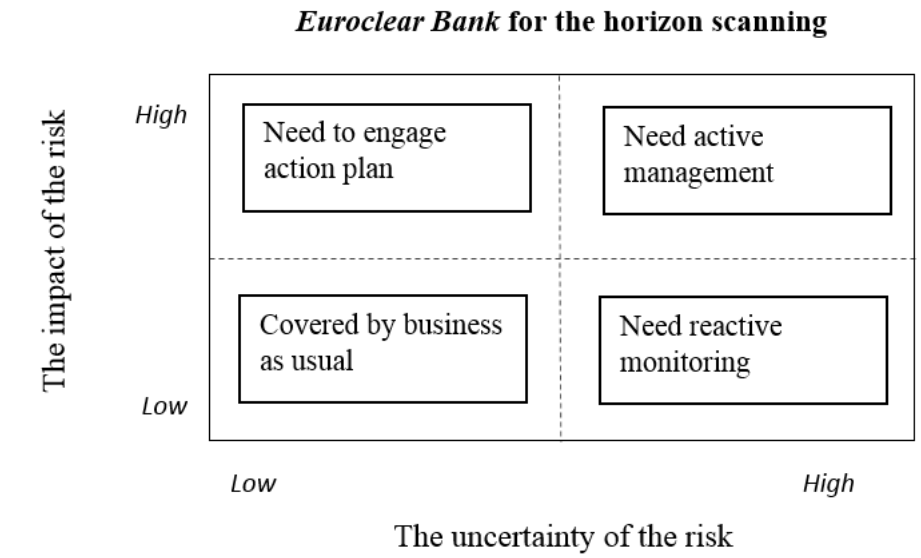
In addition, in times of crisis, the second line of defence works with the Chief Risk Security Officer (CSO) and the CEO to ensure that the right decisions are made.

Regarding the control phase, the organisation, like *Euroclear Bank*, does not use indicators. However, a crisis management procedure is planned and implemented by the crisis management teams in each country where the Operational Risk Committee acts as an intermediary between the CSO and senior management. But the final decision rests with the Chief Transmission, the director for the country concerned, or the manager if the latter is absent.

When a risk has occurred, the organisation has a backward look and evaluates its way of doing things and if there was another way that could have been put in place to avoid the possible management errors it could have made, to not make the same mistakes again.

Appendix 27: The different risk cartographies depending on one bank to another





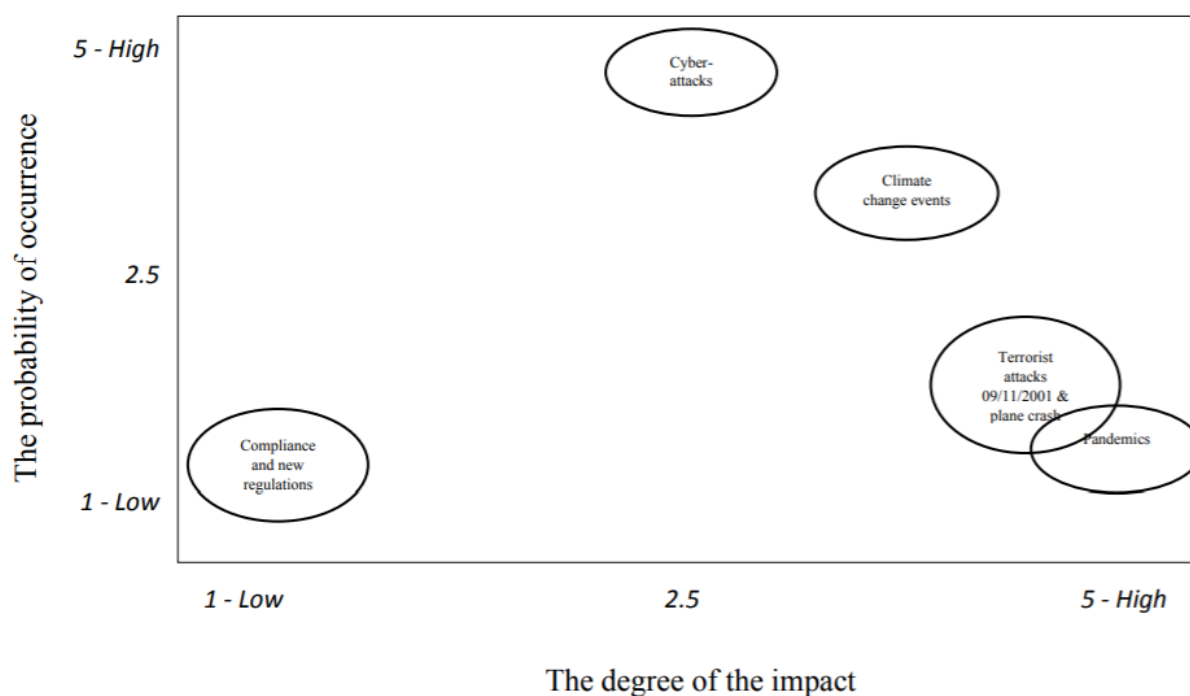
Appendix 28: This table shows how information about emerging risks is reported within the bank

	Significations
Number of times it is done	
/y	Per year
/q	Per quarter
/m	Per month
Significance of the box	
	This is not done by the banks
[blank]	The information is missing

		Type of banks							
		Large commercial banks				Small commercial bank	Investment bank	Securities clearing bank	Financial Regulator bank
		A	B	C	D				
Approach used									
To the board and to the Executive Committee	The responsible	The Risk Mgmt team	The ERM team	The ERM team	The CRO and risk department	The Risk Mgmt team	The Compliance team	The CRO	The CORO and the Mgmt team
	The type of report	‘Quarterly Risk Report’ (1/q) – ‘Top ten risks’ (1/y)		Meeting (10/y) – ‘Health Check’ (1/m or 1/q) part of the ‘Integrated Risk Report’ (8/y) – ‘New and Active Product Process’	Tutorials (as needed)		(1/q)	Workshop with the BofD (1/y)	Discussion (1/q)

				(NAPP) (2/y) – ‘Risk Scan’ (1/y)					
	The channel used	By power point presentation	By presentation – Intranet – E-learning	Orally			By a dashboard – Intranet	Power Point	
To the business line	The responsible		The ERM team	The CRO of each country or from the group (1/m)	The CRO and the ‘Single Person of Contact’ (SPoC)	The Risk Managemen t team	The Compliance team		
	The type of report				CRO talks		Discussion (1/m or 1/q)		
	The channel used		Intranet – E-learning	Emails – Internal platforms		Discussion if employees ask for	Intranet – Orally		
External approach	The responsible	The CRO and the Risk Mgmt team							
	The type of report	‘Effective leading’		The ‘Risks Signals’ (8/y)					

Appendix 29: This graph shows that in the risk assessment phase, the probability of occurrence cannot be multiplied with the degree of impact



*This matrix is based on my personal judgement and on the situation in the developed occidental countries especially in the European Union, the United States of America, the United Kingdom and Australia and is subject to interpretation.

In making it, I have taken into account some of the main emerging risks highlighted by the banks interviewed.

Moreover, the axis relating to the 'degree of impact' has been evaluated according to two dimensions: the human dimension (social loss) and the economic dimension (capital loss). The axis concerning the 'probability of occurrence' refers to the number of times during a year that these events can happen.

Firstly, regarding the risks linked to the appearance of new regulations put forward by the regulator such as those issued by the *ECB* or the *Basel Committee*. These new regulations are often the result of meetings between major international leaders such as the G20 summits or the *United Nations* with the 'United Nations Sustainable Development Goals' and are then implemented in national law. But appear rarely several times a year or once a year but rather once every five-ten year.

I am referring in particular to the three now, but soon four pillars of the *Basel Committee Agreements* which are/will be in force in 1988, 2002, 2013 and 2023. They follow major events such as the financial crisis of 2008 or the consideration of operational risks and which are the subject of a European directive applicable in every European Union law.

In addition, the *EBA* guidelines are also rare. In addition to these international regulations, there are also national regulations which aim to consider laws governing the financing of terrorism and anti-money laundering. But which also occur infrequently, compared to international laws which are more directed at regulatory capital.

These new regulations have for main impact a change in the required capital or to review the objectives and the strategy of the bank but without leading to human losses, which is why I consider these risks with a low probability and a low impact.

Secondly, concerning the risks linked to digitalisation and more precisely the possibility of cyber-attacks, many banks underlined that this happens on a daily basis with a more or less high economic impact depending on the severity of the hacking and data theft and on the possible repercussions, but again, without causing human losses.

Risks linked to climate change, on the other hand, occur more rarely than cyber-attacks, although they have become more frequent in recent years. But their impact, both human and economic, is enormous. Whether it is the forest fires in Australia in late 2019-early 2020 or those that regularly occur on the West Coast of the United States or the deadly floods that Europe experienced in mid-July 2021 and which cost hundreds of lives and left thousands homeless.

These risks, as we have seen previously, will increase in intensity in the future which explain why I rank these risks as having a medium probability of occurrence. In addition, these risks can lead to possible loss of human life among employees, the possibility of destruction of banks' data centres in locations more exposed to flooding and bad weather. But also, there is the risk that bank customers will be less able to repay their loans, which is why I rank these risks as having a high impact.

Concerning the impact of pandemics, such as the covid pandemic which we have been facing since March 2020, appearing in late November-early December 2019 in China and which cost the lives of more than 4 million people worldwide. The banking sector was not particularly affected by the crisis from an economic point of view, no doubt due to the digitalisation of its services and products, the impact is nonetheless significant, both in terms of human losses and in terms of the reaction that banks had to adopt, as a result of the drop in the liquidity level of their clients and their ability to repay their debts, but also thanks to the support to the affected sectors.

Finally, terrorist attacks such as those of 11 September 2001 had a huge impact on the financial market, which led to the bursting of the Internet bubble and increased the debt of the United States and damaged its economy through a drop in tourism and visitor numbers. As a result of which the US Federal Reserve adjusted its interest rate policy, which explains the significant degree of impact, not to mention the loss of life. Our European Union countries have also suffered enormously from terrorist attacks in 2004 in Madrid, 2015 in France and 2016 in Brussels.

In addition, *World Bank* had, in the interview, described aircraft crashes as an emerging risk for them, following the crash of the Ethiopian Airlines Boeing 737 Max in 2019 which resulted in the death of twenty *UN* staff and one *World Bank* staff member on their way to a conference. As a result, *World Bank* has become acutely aware of the importance of not putting all of its staff on the same plane to avoid possible high impact that this can have on the organisation in case of loss of qualified staff.

Nevertheless, it is a fact that aeroplane crashes occur several times a year. In 2020 alone, seven aeroplane crashes were recorded, as was the case in 2019, resulting in the death of more than 300 people. In addition, there is the economic cost of compensating the families of the victims for the loss of life.

The event	Probability of occurrence (value in numbers)	Degree of impact (value in numbers)	Total results (value in numbers)
Compliance and new regulations	1.00	1.00	1.00
Cyber-attacks	2.50	5.00	12.50
Climate change events	3.50	3.50	12.25
Pandemics	5.00	1.00	5.00
Terrorist-attacks and plane crashes	4.50	2.00	9.00

Finally, if I apply the method according to which the quantification of a risk is calculated by multiplying the probability of occurrence and the degree of potential impact, this would mean that cyber-attacks and risks related to climate change are more important than the risks of pandemics, terrorist attacks, airplane crashes and new regulations for banks. Nevertheless, the organisational and economic effects of these risks cannot be considered as the same for banks.

Indeed, in the case of a plane crash, the bank may see a risk of losing its human capital but with limited financial consequences. While pandemics, new regulations and climate change lead to more economic losses, whether it is inflation, and the impact on the financial market, inability to repay loans or changes in investments. Terrorist attacks, on the other hand, have considerable impacts on both social and economic capital.

