City Research Online

City, University of London Institutional Repository

Citation: Nunes, Paulo (2014). Holistic risk management in commercial air transport. A methodology to apply ISO 31000 to the airline industry. (Unpublished Doctoral thesis, City University London)

This is the accepted version of the paper.

This version of the publication may differ from the final published version.

Permanent repository link: https://openaccess.city.ac.uk/id/eprint/13571/

Link to published version:

Copyright: City Research Online aims to make research outputs of City, University of London available to a wider audience. Copyright and Moral Rights remain with the author(s) and/or copyright holders. URLs from City Research Online may be freely distributed and linked to.

Reuse: Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge. Provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.

City Research Online: http://openaccess.city.ac.uk/ publications@city.ac.uk

Holistic Risk Management in Commercial Air Transport

- A methodology to apply ISO 31000 to the airline industry -

Thesis submitted for the award of Doctor of Philosophy (PhD) in Air Transport Management

by Paulo Nunes

Lead supervisor:

Prof Roger Wootton FREng.

City University London

School of Engineering and Mathematical Sciences

October 2014

– Intentionally left blank –

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AIRMIC	Association of Insurance and Risk Managers
ALARM	The National Forum for Risk Management in the Public Sector
AS/NZS	Standards Australia / Standards New Zealand
COSO	Committee of the Sponsoring Organisations of the Treadway Commission
EASA	European Aviation Safety Agency
ECGI	European Corporate Governance Institute
EIU	Economist Intelligence Unit
ERM	Entreprise Risk Management
FAA	Federal Aviation Administration
FERMA	Federation of European Risk Management Associations
FRC	Financial Reporting Council
G31000	The Global Platform for ISO 31000
IATA	International Air Transport Association
ICAO	International Civil Aviation Organisation
IMA	Institute of Management Accountants
ISO	International Standards Organisation
KPI	Key Performance Indicators
RIMS	The Risk Management Society
RM	Risk Management
SEC	Securities and Exchange Commission
WEF	World Economic Forum

– Intentionally left blank –

Acknowledgements

Life has its ups and downs. A banal statement, most certainly, yet everyone has gone through phases of enthusiasm and periods of gloom in life. An academic challenge such as writing a doctoral thesis is similar. Over the years that it took to align the methodology, find cooperation partners, collect all information, produce a solid proposal, have it validated, and in parallel write the thesis, I have suffered many moments of frustration and anguish, but also enough positive periods motivating me to keep striving ahead. Never loosing the ultimate goal of sight was certainly the main challenge. Achieving the end of this process is, though, a rewarding moment. Even if it has proven to be a very solitary work, it could never have been achieved without the constant support by a lot of different people. Their invaluable contribution must be humbly recognized.

A first word of appreciation goes to my family. You have always been there for me, supported my efforts to overcome every hurdle and were patient with me during moments of frustration. Thank you for allowing me all the conditions to proceed with this endeavour. Over this long time, all of you encouraged me - in your own ways - to pursue this goal. I share this moment of joy with all of you.

A big ‘thank you’ goes, of course, to my supervisors: Prof. Roger Wootton and Dr. Pedro Pinto. Roger, you launched me this challenge a long time ago, even if at first I was reluctant to continue with any academic research activities. You always believed in my capacity to achieve solid results and kept pushing me until I met my objectives. The bar was always set high, but I hope I managed to meet your expectations. Thank you for guiding my academic progress over the past decade, from MSc-times till today. Pedro, your constant support, experience and guidance was priceless. Having you as local counterpart was essential to keep steering my work to the right direction especially in moments of distress and discontent. I am sure I could not have achieved the end without your help.

Nuno and Teresa, bright guiding lights in the Polar Regions: my life wouldn’t be as fun without you. Your friendship and endless ability to listen are pillars of strength. Teresa, your creativity and thought provoking questions inspired me to always think twice on every angle and approach I used. True value was added to my work with all our discussions. I wish I could return in the same manner. Nuno, thanks for always cheering me up when darkness threatened to fall upon me. You have been a true companion on these roads of gravel and

slippery ice. May the force be with you! I owe you both something truly holistic: say a big portion of *secretos de porco preto* followed by a few *ginjinhas* at our favourite restaurant?

Thanks also to Sascha Feuerherd and Dr. William Gibson, not only for comments made throughout the work, but especially for allowing me the flexibility to accommodate professional obligations into the tight academic research and reporting schedule.

This work could also never have been achieved without the contribution of all those personalities who where available for multiple interviews, e-mail discussions and face-to-face meetings, actively feeding this thesis with their knowledge and experience.

I should also thank all of those that never replied to e-mails and invitations to contribute or broke own promises to cooperate. It is always possible to learn as much from the words that are said as from those that are never outspoken.

Abstract

Risk became popular among management theorists, with many proposing ways to manage all sorts of risks. Some countries require corporations to implement risk management as stand-alone or even integrated element within improved internal control frameworks. As result, several national standards were developed over the last 20 years, but just one arose as truly international solution: ISO 31000.

Little has been published on integrated risk management at airlines and the use of industry-wide standards has never been consistently explored before. Two industry-specific standards exist, but their limited scope led to little adherence by airlines. To cover this gap, this thesis analysed the wider picture of integrated airline risk management practices, aiming at identifying improvement areas to propose an adaptation of the ISO 31000 risk management framework.

Several empirical methods (including a survey to publications by the Top100 airlines, and interviews to airline risk managers, experts and practitioners) showed that only six airlines reported using ISO 31000, with two others citing its predecessor, AS/NZS 4360. Many vaguely referred to COSO, customised models or didn't mention any framework.

It is unclear why only few airlines use ISO 31000, when other industries applied it successfully before. Therefore, to help disseminating ISO 31000 among airlines, a customised framework has been designed that proposes a truly holistic industry-specific approach, not focussing on individual risk sources. It integrates risk management along the airlines' entire value chain and involves relevant stakeholders in the airlines' internal risk management efforts.

The proposal's validation process showed that, while being ambitious in its goals, the customised framework is complete and concise, providing valuable input for airlines using other risk management models. It has been considered particularly suitable for those airlines thinking of launching risk management initiatives. Given that a fundamental culture change is needed, the timeframe for implementation should be generous, allowing for several process iterations and revisions.

– Intentionally left blank –

1. Introduction & objectives

The present thesis develops the topic of risk management at commercial air transport operators (focussing the work on airlines only, not other involved entities – airports, air traffic control, business jet operators, air taxis, etc.), while discussing the current state-of-the-art and proposing improvements when and where applicable. Before launching the discussion on conclusions achieved and proposals designed during the various work steps, it is important to well define the starting point that triggered this whole exercise. Therefore, this first chapter of the report will set the basics by describing the context in which the thesis' topic has been conceived, what the main problem statement is and what the associated research questions are, ultimately explaining what the core objectives are (and what it is not intended to cover and achieve). The document structure will be briefly addressed, showing that the topic has been approached from a bottom-up perspective, starting with the generic understanding of the key subject (risk and risk management) before diving into industry-specific applications and uses (risk management at airlines).

Anticipating what will come in a later chapter, and in order to avoid any misinterpretations, the definitions of risk and risk management adopted for the purpose of this study are sourced from the Vocabulary Guide 73, base to ISO 31000:2009, the most recent and internationally recognized standard for risk management developed by the International Organisation for Standardisation (ISO).

Figure 1: Definition of Risk

Risk "effect of uncertainty on objectives"

Source: (International Organisation for Standardisation, 2009c, p. 1)

Figure 2: Definition of Risk Management

Risk Management "coordinated activities to direct and control an organisation with regard to risk"

Source: (International Organisation for Standardisation, 2009c, p. 2)

As it is the most recent and wide spread standard, many other of its definitions and concepts shall be used throughout the text.

1.1. Context description

Any business at any time faces internal and external challenges that might constitute risks to its existence. These can be of various origins (operational, financial, technological, political, etc.), diverging scales (local, regional, global) and durations (short-, mid- or long-term). They require strategic and tactical responses so that the organisation is prepared to face the specific risk, if and when it happens. History has shown that the concentration of management efforts is mostly on the short-term only, removing the long-term strategic thinking that is required to manage the organisation sustainably over time.

Without surprise, the airline industry suffers from the same symptoms. Mr. Kichisaburo Nomura, former Chairman of the Board of ANA All Nippon Airlines, stated in 2003 that "enterprises, including ANA have so far basically coped with risks on a case-by-case basis. Individual response sounds better, but the problem is that it achieves only partial optimization and not total optimization and that there have potentially been remaining risks that have gone unrecognized"(Nomura, 2003, p. 469).

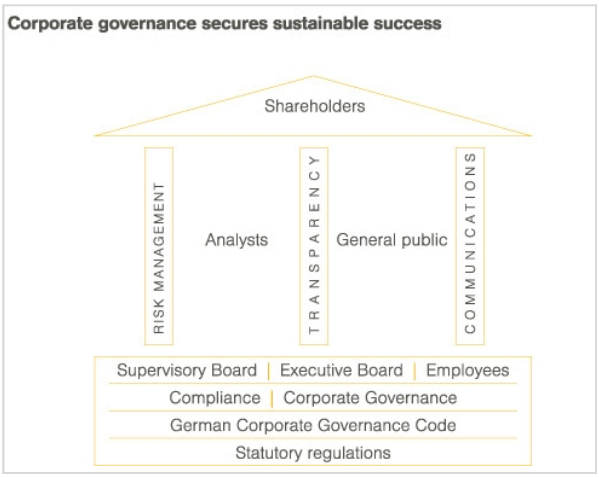
So, taking this statement as example, also airlines were looking at risk management from a compartmented perspective only, instead of using a systemic and global approach.

ANA introduced a formal Risk Management process in 2002, with the timing of this decision being no surprise: it was an immediate response to the September 2001 terrorist attacks in the USA and the spread of SARS in Asia in 2002. Also Singapore Airlines launched their formalised Risk Management Framework in 2002, other airlines followed these footsteps.

In the past 20 years the world has evolved into a deeper and ever closely knit net where one isolated cause at one end provokes a variety of effects at another end. Political instability, technology, environmental concerns, stakeholder expectations and infrastructure shortcomings are just examples. The list of impact factors is endless and each individual issue assumes different weights for each organisation, depending on a variety of other factors such as its nature, geographical location, business strategy or even its specific cultural and economic environment. This is all more valid for global industries such as air transport. Managing the full complexity of an airline's internal and external environment has therefore become a continuous test even to experienced chief executives and managers, where no off-the-shelf formulas or textbooks can give full answers.

More and better information is required coupled with new evaluation techniques and improved tools to take effective decisions with long-lasting results. Therefore Lufthansa German Airlines has inscribed 'Risk Management' as one of the key pillars of its corporate governance model. Nevertheless, it should be stressed that the system underneath is called "Opportunity and risk management system", opening the door to grasping upsides of challenges – not only their threatening aspects.

Figure 3: Lufthansa Corporate Governance Model



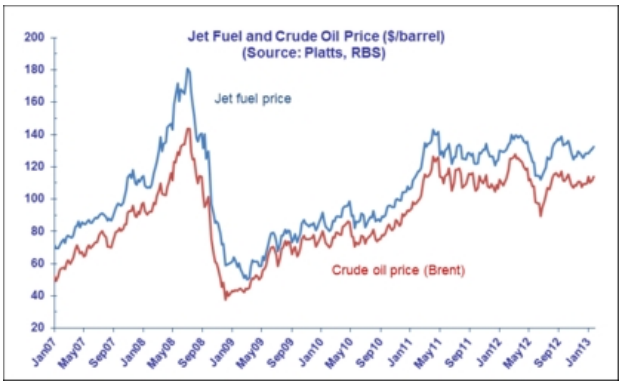
Source: (Lufthansa German Airlines, 2013)

But how are other airlines doing it? Is Enterprise Risk Management (ERM) a common practice in this industry? How has the perception of risk evolved over the past years? And what resources are required to introduce an effective ERM model even at smaller airlines?

The focus of this project is thus going to be risk management in the airline industry, in order to understand what has been done so far by airlines to cope with the ever increasing risk landscape. It is intended to assess how effective these measures have been and understand what other and better ways are possible to manage risks, learning lessons from other industries.

In areas related to operational and financial risks, airlines have already implemented means to measure and guide decision-making towards risk mitigation. Beyond covering only a limited part of the total risk landscape, their full effectiveness can be questioned. As example, fuel hedging was a traditional cash saver for airlines, but it resulted in losses as soon as the fuel price showed unusual volatility, sharply rising and dropping in value in just a few months in the year of 2008.

Figure 4: Jet fuel price development 2007-2013



Source: (IATA, 2013a)

Christopher Pratt, Chairman of Cathay Pacific, stated in the companies' 2008 Annual Report: "The fall in fuel prices, though welcome, caused unrealised mark to market losses of HK$7.6 billion on our fuel hedging contracts for the period 2009-2011 which were entered into in order to give a degree of certainty as to future fuel prices and protection against price increases. Our associate Air China also incurred unrealised mark to market losses on fuel hedging contracts and a provision of HK$1 billion has been made covering fourth quarter losses" (Cathay Pacific, 2009, p. 6).

Singapore Airlines suffered a 43,8% increase in fuel costs in its 2008-2009 financial year, accumulating a loss of US$306 million due to their fuel hedging policies. Nevertheless, Stephen Lee, Chairman of Singapore Airlines, stated that "Singapore Airlines always adheres to a prudent – some even say conservative – strategy on fuel hedging. So what we lose on those hedges, we can offset with gains against our budget price for fuel that we did not hedge, as the price falls" (Singapore Airlines, 2009, p. 6).

Was it bad forecasting, bad tools, automated decision making lacking critical judgement or even all the above combined?

In other areas, companies tend to trust insurances to cover for potential risks. But what about those risks which are not insurable and by definition beyond the management's control? What is the best approach for these?

It is also understood that there are risks that affect the global aviation industry (and therefore all airlines; although some risks are outside of an individual airlines' own control), yet the way that each individual airline perceives and manages this risk is different. Therefore should each airline have its own (or none?) risk management model? An

additional element of this project is to understand what guides risk management at each airline and what limits or constraints its applicability.

As mentioned above, there should be no silo approaches, always embracing the full spectrum of risks affecting the aviation industry in global and each airline in particular. Therefore, the scope of this study is intended to be broadened to the strategic and holistic level, not limiting the areas to "just" operations or finance, but the airline as a whole.

1.2. Problem statement

Given this complexity and number of reasonable questions that arise from it, the core problem statement for this project has been defined as follows below.

Figure 5: Problem statement

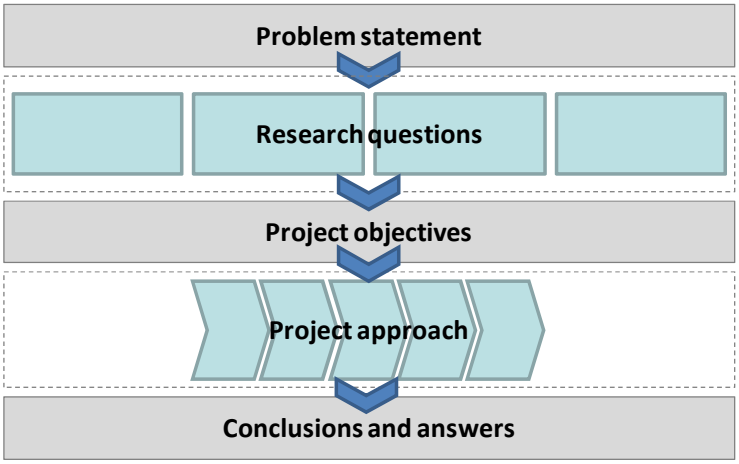
Verify the convenience and feasibility of introducing a common risk management model in commercial air transport operators and, if affirmative, identify best practices and standards to help them mitigate the different risks they face.

This problem statement by itself opens doors to another set of underlying topics:

- Is it convenient to introduce a risk management model at airlines?
- Is it feasible to do so?
- Can such a model be common to all airlines?
- Can such a model be made specific to commercial air transport operators?
- Are there any relevant best practices and standards that can serve as guideline?
- Can these help mitigate risks faced by airlines?

The accurate definition of this problem statement is the true starting point to the project, enabling the creation of a conducting line throughout the entire exercise. It is around this problem statement and underlying topics that a number of separate and independent, yet more focussed research questions and project objectives have been designed (see next sections of this chapter). To achieve these, a phased approach and methodology has been adopted, as described in Chapter 3 that develops the various work packages, answering the previously listed research questions and the overall problem statement. The figure below depicts this project framework.

Figure 6: Problem statement and project framework



1.3. Research questions

Four major research questions have been identified that will, if and when answered, help solving the overall problem statement and underlying issues. Each research question can be divided into further sub-questions in order to get a more detailed and granulated answer to the initial one.

Figure 7: Research questions

Therefore, for each of these research questions the respective sub-questions are:

1. What is current practice in airline risk management?
   - Is comprehensive risk management a common practice at airlines (or even understood and wanted by higher management)?
   - How much of the internal and external environment is really known, managed and controlled by an airlines' management?
2. What processes and resources are used?
   - What processes do airlines apply to identify the risks surrounding its business?
   - How do airlines identify, distinguish and manage risks that are common to the industry and those that are unique to its own business?
   - What tools and techniques are available to manage all these risks and are they effective?
3. Are there improvement areas?
   - Is there a common industry-wide approach or is each airline following its own process?

- Are “what if” scenarios and “what to do when” portfolios realistic for smaller scale airlines?
- How do insurance companies understand risk management at airlines and can they play a bigger role in the risk management process?

4. How should an airline-specific model be?
   - What would be an ideal risk management model for a smaller airline, with fewer resources?
   - Is there any lesson to be learned from other industries?
   - Is ISO 31000 applicable to commercial air transport, as the latest risk management standard?

Despite the ambitious starting point, it is expected that not all of the above sub-questions can be thoroughly answered within the scope of this project. Several reasons contribute to this expectation:

- General information and data accessibility. Existing reports and primary information sources to be used may not be available and/or provide full disclosure.
- Time limitations. Given existing timelines to be complied with, data and information might not be accessible in a timely manner.
- Barriers to entry. Despite all efforts, the chosen industry and/or representative industry associations might reject attempts to improve its current processes, therefore block access and close opportunities to elaborate proper research.

1.4. Project objectives: inclusions and exclusions

Answering the above research questions is of course the first and major objective of this project. Nevertheless, there are a number of other secondary objectives – potentially of a more high level nature – than the mere answering of those initial questions. Therefore, this project aims at the following:

Figure 8: Project objectives

- Answer as many research questions as possible;
- Expand knowledge in the field of enterprise risk management;
- Cover existing gaps in industry-specific literature on the subject;
- Provide usable input for the airline community;
- Propose a model that combines the best of available industry-neutral standards and industry-specific features;
- Launch a wider debate on possible next steps to implement industry-specific risk management practices.

As will be visible throughout the next chapters, this project is not about any individual risk identification, analysis, evaluation and treatment methods and tools. It will therefore not focus on one or other risk individually, nor on what airlines are doing to mitigate it, rather focus on the underlying process used (if any) by airlines to identify the vast variety of risks they are exposed to, regardless of their nature. It will not cover flight or ground operations, safety aspects, fuel price issues, natural hazards or meteorological events, supply chain issues or any other specific item – as relevant as it is, that would be treating the integrated risk management approach from a silo perspective. The focus will be on the integrated approach and process used by this industry to identify their broad risk landscape, what and how these are evaluated, assessed and treated. Given all this, this project will add another layer of knowledge to existing studies and proposals, empirically testing a suggestion on how to design a broad risk management approach at airlines.

1.5. Document structure

The present document reflects the various stages of the work performed and has been structured in a manner consistent with a step-by-step construction of the arguments towards reaching the final conclusions.

The figure below depicts the key elements to be addressed in each chapter.

Figure 9: Document structure

Description		Contents
Chapter 1	**Introduction & objectives**	Set the basics: describe origin of the topic, context, research questions and objectives.
Chapter 2	**Literature review**	Gather relevant concepts and information on the core subject from existing publications.
Chapter 3	**Methodology & approach**	Outline the individual work steps to be performed during the research.
Chapter 4	**Available Risk Management Standards**	Describe and critically evaluate validity and applicability of existing standards.
Chapter 5	**Current Risk Management practices at airlines**	Detail findings from individual work steps dedicated to collecting information from airlines.
Chapter 6	**Discussion and identification of improvement areas**	Debate possibilities of improving and/or adapting existing models to airlines.
Chapter 7	**Designing a new model for commercial air transport**	Propose a new industry-specific model using the findings from previous work-steps.
Chapter 8	**Testing proposition**	Check the validity of the proposed model and explore respective improvement potentials.
Chapter 9	**Discussion of results achieved**	Summarize all findings to answer research questions outlined in Chapter 1.
Chapter 10	**Conclusions and recommendations**	List conclusions and contributions of work performed and explore ways for further research.

This first chapter establishes the starting ground for the research project opening the way towards answering the key problem statement. Chapter 2 summarises the most important concepts on the core subject of risk management from available literature. Based on these, Chapter 3 describes the methodological steps and overall approach that have been adopted to address the work at hand. Currently available risk management standards, both industry-neutral and industry-specific, will be addressed in Chapter 4, discussing their advantages and disadvantages in the current airline risk management environment. Chapter 5 will detail the findings of the individual work steps conducted during the research phase (as described in Chapter 3 Methodology & approach); these are further discussed in Chapter 6, highlighting gaps and overlaps thereof and the resulting need for an industry-specific risk management model. Chapter 7 elaborates on such a new model, its relevance and application possibilities. This model is then subjected to a validity testing, whose results are presented in Chapter 8. Chapter 9 reviews the overall result achievement discussing if project objectives have been achieved and research questions answered. Chapter 10 will close the entire document, outlining conclusions and suggesting areas for further research.

– Intentionally left blank –

2. Literature Review

Discussing risk management strategies implies, first of all, a good understanding of what risk is. While this chapter is not intended to rewrite the whole history and origin of risk, its definitions and theory[1], it will firstly present key concepts that have been considered relevant for this study[2]. Cultural aspects will be addressed, before presenting definitions for risk appetite and discussing the importance of this concept in risk management.

Over the past decades, the world has witnessed the rise and evolution (or fall and extinction) of many management theories and practices. Risk management is one of those theories: it has grown in importance, becoming a wide-spread activity, yet companies still fail regardless of the industry they are working in or their geographical location. Even if this study is not aimed at discussing the many reasons that lead companies to fail, some questions can and should be asked: do they fail because they do not understand what risk is or is there a fundamental lack of proper risk management? Or, on the other hand, do they fail because their risk management process failed? Or, if they had good risk management, was there poor decision making (thus management) involved?

So another topic to be discussed in this chapter is why risk management fails and what the key ingredients for good risk management are (if they exist). This will enrich the discussion trying to answer the ultimate question if risk management is a science or an art.

2.1. The concept(s) of risk

If taken from a historical perspective, the bridge between current risk management models and the origin of the first risk definition extends over several centuries. Peter Bernstein goes back to the times of the ancient Romans, Greeks and Arabs, to justify the initial steps of the evolution of what we now know on risk. He says “the word ‘risk’ derives from the early Italian *risicare*, which means ‘to dare’. In this sense risk is a choice rather than a fate. The actions we dare to take, which depend on how free we are to make choices, are what the story of risk is all about” (Bernstein, 1996, p. 8). Ulrich Beck says: “the Greeks understood that more things might happen in the future than actually will happen” making reference to several Greek philosophers such as Plato and Aristotle (Beck, 1992, p. 43).

[1] There is already a range of books that cover this topic in enough depth to get the full historic view on the subject, e.g. (Bernstein, 1996) and (Beck, 1992).
[2] The herein covered literature includes publications up to December 2013.

From another perspective, Beck defines risk as “a systematic way of dealing with hazards and insecurities induced and introduced by modernisation itself” (Beck, 1992, p. 21). He suggests that risk and society evolved so much that we are living in a risk society where risk is a result of modernization.

In more recent literature, notably The Orange Book published by the HM Treasury in 2004, risk is defined as the “uncertainty of outcome, whether positive opportunity or negative threat, of actions and events. The risk has to be assessed in respect of the combination of the likelihood of something happening, and the impact which arises if it does actually happen” (HM Treasury, 2004, p. 9) opening doors to risk likelihood and assessment as part of the risk management processes. This comes as consequence of the introduction of several risk management standards, such as the pioneering AS/NZS 4360:1995 standard launched by the Australian and New Zealand Standards Commissions. (More on standards can be found in Chapter 4 Available Risk Management Standards.)

And yet risk and uncertainty are conceptually different things. Douglas Hubbard defines uncertainty as being “the lack of complete certainty – that is, the existence of more than one possibility. The ‘true’ outcome/state/result/value is not known”; whereas risk is defined as “a state of uncertainty where some of the possibilities involve a loss, injury or catastrophe, or other undesirable outcome” (Hubbard, 2009, p. 80). John Adams simplifies: “if you don’t know for sure what will happen, but you know the odds, that’s risk; and if you don’t even know the odds, that’s uncertainty” (Adams, 1995, p. 25).

What must be recognized, though, is that every individual (and organisation) willingly takes risks. Further in his comments, John Adams states: “the single-minded pursuit of a zero-risk life by staying in bed would be likely, paradoxically, to lead to an early death from either starvation or atrophy. There is no convincing evidence that anyone wants a zero-risk life – it would be unutterably boring” (Adams, 1995, p. 15). This assumes of course that the bed (and the bedroom, the flat or house, in that particular neighbourhood, city and region) would be the safest and risk-freest place of all, where nothing bad could happen. And yet that is not true either, so in reality there is no such thing as a risk-free place, let alone a risk free life.

This is where Adams introduces two further concepts: the risk compensation and the risk thermostat as responses to risk. The risk compensation model reflects the balancing behaviour of each individual towards all risks. It links the propensity of taking one particular

risk with the obtainable rewards, based on the perceived danger. This balancing act is what Adams compares to a "thermostatically controlled system" where each individual has different sensitivities, making risk evaluation a highly subjective process. And as no individual lives without other human interaction, risk becomes interactive and risk perception evolves with the input and exchanges with other individuals. It is a revolving system where the valuations, opinions and feelings of one individual may (or will) influence those of another individual. Extrapolating, an entire society or organisation may be assessing a risk from a specific perspective given the many subjective contributions to its valuation. This justifies the desperate need by some authors to produce quantitative analysis and introduce rationality, in an attempt to simplify something that is intrinsically complex and unquantifiable.

Adams further presents the characteristics of the *homo prudens* versus the *homo aleatorius*, the two opposite descriptions of what an individual can be when facing risk, based on the traditional wisdom of 'to err is human'; and yet so is 'to gamble'. Ultimately both characteristics are present in every individual, although the moment of externalisation of one or the other facet and its intensity varies from person to person. While *homo prudens* represents the zero risk man, *homo aleatorius* is the ultimate expression of an individual willing to take all risks, underlining the 'no risk, no reward' attitude in so many quadrants of modern society. "*Homo prudens* strives constantly, if not always efficaciously, to avoid accidents. Whenever he has an accident, it is a 'mistake' or an 'error'" (Adams, 1995, p. 16), trying to learn from those unwanted accidents and introduce changes to its future production and decision making processes. On the other hand, the *homo aleatorius* is a consequence of a "society that glorifies risk". Where would the world be if no inventor had ever tried a new approach to a problem or no entrepreneur had ever taken risks when launching a new venture? "We respond to the promptings of *homo aleatorius* because we have no choice; life is uncertain", the author concludes (Adams, 1995, p. 17).

These few statements concentrate all elements of what risk is and how it can be managed:

- Risk depends on individual judgement; it is therefore subjective and volatile as the opinions, valuations and circumstances of each individual also evolve.
- The perception of risk changes over time, not only because of its evaluators' own evolution and the input received from third parties, but also because the evolution of each risk item itself: what is considered to be a risk on one day might vanish over the next days. It is, thus, no surprise that some authors claim 'wait and see' is sometimes the best attitude to face a specific issue.

- Therefore risk involves the probability of something happening (or not), and hence leading to the need for measurement of that probability level – yet quantitative analysis alone has proven to be insufficient (see next sections).
- But measuring alone is not enough to have a risk covered: a decision is required to take one or another mitigation action and sometimes the missing decision from one (potentially risk averse) individual hampers the overall process.
- Risk is infinite and varied in numbers, nature, origin and potential consequence; full control of all risks (100% *homo prudens*) is impossible, yet living without a single risk mitigation action of whatever sort (100% *homo aleatorius*) isn't sustainable either.
- Therefore knowledge and information becomes essential to evaluate, qualify and ultimately manage each individual risk as such and as part of an overwhelming risk landscape.
- Minimising consequences of a particular risk, if it really happens, should be the ultimate goal.

All the above can easily be brought to entrepreneurial level: ultimately companies are made of people. Decisions have to be taken every day, at all organisational and functional levels, regardless of how big or small that decision might be, even when there is incomplete information or time pressure to advance.

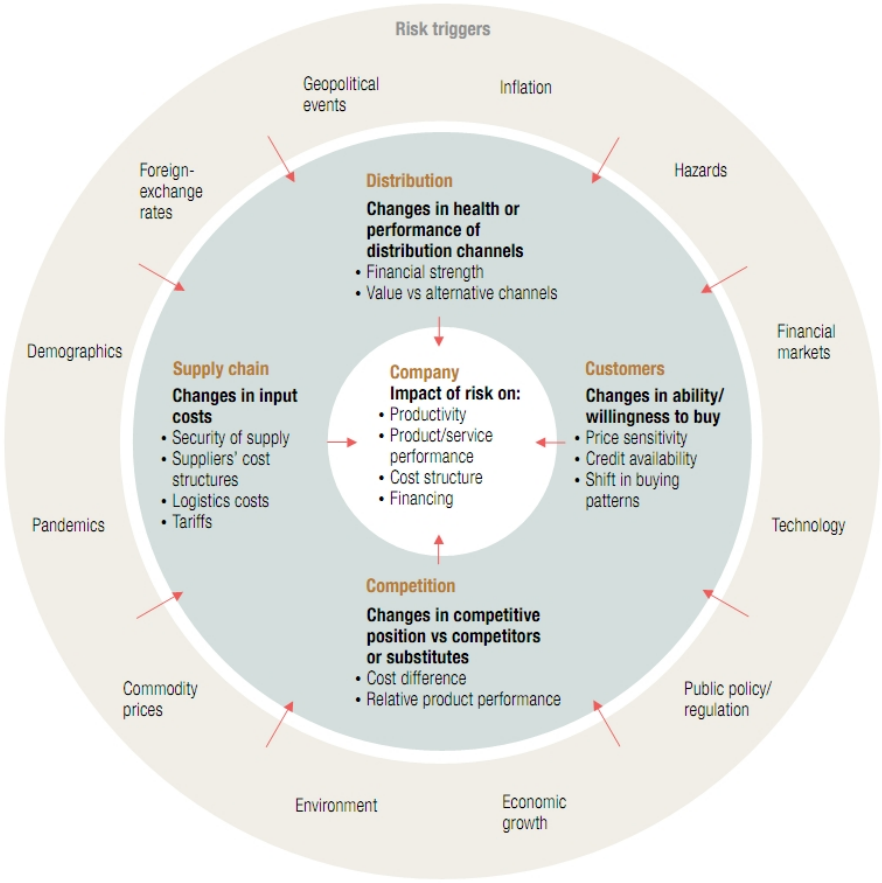
But, in the words of Nassim Nicholas Taleb, the world is random, hence uncontrollable. Yet, "we have a hunger for rules because we need to reduce the dimension of matters so they can get into our heads. [...] The more random the information is, the greater the dimensionality, and thus the more difficult to summarise. The more you summarise, the more order you put in, the less randomness. Hence the same condition that makes us simplify pushes us to think that the world is less random than it actually is." (Taleb, 2007, p. 69). But it is not, and by simplifying we actually eliminate information from our visibility screen, therefore creating what Taleb defines as 'opacity'. And what falls out of the simplification process – what is not visible – is what Taleb has defined as the black swan, the uncontrollable, unforeseen and unaccounted for event. So we don't know everything, regardless of how much one strives to further increase knowledge. And yet, "we tend to use knowledge as therapy" he says (Taleb, 2007, p. 69). Even so, life must go on, fully conscious about its randomness.

Researchers from McKinsey & Company, a strategy consulting firm, elaborated on a further concept: cascading risk. They suggest that there are risks beyond an organisations' sphere of influence and visibility (and therefore knowledge). "Risks gone bad in one part of the economy can set off chain reactions in areas that may seem completely unrelated. [...]

Most companies have some sort of process to identify and rank risks, often as part of an enterprise risk management program. While such processes can be helpful, [...] they often examine only the most direct risks facing a company and typically neglect indirect ones that can have an equal or even greater impact" (Lamarre & Pergler, 2009, p. 2).

The figure below illustrates this concept. While the company is at the centre, being influenced by its supply chain and its direct environment (formed by all possible stakeholders), there may be risks in the outer rim, where visibility and knowledge are limited. This potential risk is beyond the companies' control.

Figure 10: Cascading risks



Source: (Lamarre & Pergler, 2009, p. 3)

A practical example on this cascading risk concept is the case with bread prices in summer 2010. Reports on its steep price increase surged from all over the world at a time when Russia was facing a summer of draught and forest fires. There are estimates that 20% of Russia's wheat fields have been destroyed. To avoid internal supply chain disruptions and food price increases, Russia banned all grain exports on August 5th 2010, becoming effective from August 15th until December 2010. "Russia is the world's No. 3 wheat

producer and its crop loss has caused the price of wheat to almost double since June" (Miller, 2010).

This is underpinned by the evolution of the price of wheat, shown below, at the Chicago Mercantile Exchange, the world's leading derivatives marketplace, where within a few weeks the price of wheat increased more than 80%.

The chain of events is simple: one of the biggest producers reduces the production and hence supply of wheat to international markets, global demand forces prices to go up. Until the flour reaches the bakery and bread the consumer, the final product has suffered several price increases, ultimately leading to a reduction or readjustment of demand by the consumer. From an individual bakery's perspective, nothing can be done against forest fires in Russia, let alone wheat price negotiations at global stock exchanges. Even if one particular bakery has a risk management process in place, including futures and option contracts for wheat prices, it is unlikely that the impact of forest fires in Russia has been accounted for.

Figure 11: Wheat price evolution May-August 2010

Source: (CME Group, Inc., 2010)

Similar examples could be made for other industries, including of course air transport. Yet, considering that all risks are covered just because there is a risk management process in place is probably the first mistake in any such process. It is impossible to know, let alone manage, all that can affect a companies' future. It is therefore always recommended to have an approach as broad as possible when it comes to risk management. But before presenting alternative risk management models, the next section will discuss some cultural issues about risk as means to complement background and conceptual information on risk.

2.2. Cultural aspects on risk

In line with what has been discussed above, risk is viewed by many authors as a cultural or even religious issue, not just in the strict sense of regional or national characteristics, but rather in the full context of values and beliefs each individual is educated in. Adams says "we hear and see only information that gets through our cultural filters. The perception of, and concern about, risks is volatile. What gets through a cultural filter is often a matter of emphasis and presentation" (Adams, 1995, p. 86). Therefore two individuals can have, when confronted with the same situation, completely opposite reactions given their own cultural background.

Bernstein goes further: "few people feel the same about risk every day of their lives. As we grow older, wiser, richer, or poorer, our perception of what risk is and our aversion to taking risk will shift, sometimes in one direction, sometimes in the other. [...] Time changes risk in many ways, not just in its relation to volatility" (Bernstein, 1996, p. 263).

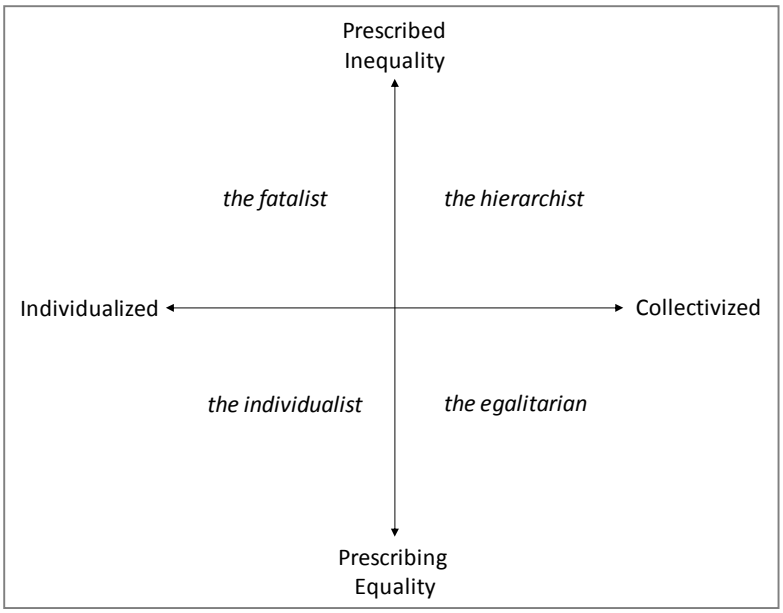
Sociologists have discussed the meaning and value of time in different cultures. Mary Douglas and Aaron Wildavsky come to the conclusion that "nothing influences the estimate of probabilities more than the sense of future time. Most people conceive the future as a straight extension of the present, but there are large variations" (Douglas & Wildavsky, 1992, p. 85) transforming decision making into either a stressful activity or a relaxed one depending on the social context the individual and/or the organisation is living in.

Douglas and Wildavsky dedicated an entire book to 'Risk and Culture' (published the first time in 1983, republished in 1992), exploring such issues as risk origin and treatment in various cultural contexts and presented their thesis along buzzwords such as 'risks are hidden', 'risks are selected', 'assessment is biased' and 'risk is a collective construct'. In this context they present the problem of choice, when facing various alternatives. "Choice between important issues has moral implications. Choice is about the future. [...] Adding more data will not always make the choice easier. Some parts of the question have to be put in the shade so as to highlight a more manageable choice between losses and gains" (Douglas & Wildavsky, 1992, p. 85). And so, not only is the concept of morality different for each individual, but also by excluding some parts of a problem to make better choices, each individual is already making a conscious choice.

Further on these authors present four different methods for risk assessment, although they immediately accept that "each method is biased" (Douglas & Wildavsky, 1992, p. 71).

Adams, on the other hand discusses four 'myths of human nature' or personality features that distinguish each individual when looking at risks: the fatalist, the hierarchist, the individualist and the egalitarian (Adams, 1995, p. 36). He displays a graphic visualization along two axis (below), where one depicts less individualistic or more collectivistic types, while the other reflects individuals constrained by restrictions on choice by superior authority (prescribed/inequality) or no externally prescribed constraints on choice (prescribing/equality), "where people negotiate rules as equals as they go along".

Figure 12: The four myths of human nature



Source: (Adams, 1995, p. 35)

In summary:

- *the individualist*, "are enterprising 'self-made' people, relatively free from control by others, and who strive to exert control over their environment and the people in it." Adams suggests that accumulated wealth and number of individuals under their control are measures to assess the success of each individualist.
- *the hierarchist*, respects the existing strong group boundaries. "Social relationships in this world are hierarchical with everyone knowing his or her place". Examples could be low rank military staff and civil servants.
- *the egalitarian*, has "strong group loyalties but little respect for externally imposed rules, other than those imposed by nature. Group decisions are arrived at

democratically and leaders rule by force of personality and persuasion." Religions, sects and environmental groups are cited herein.

- *the fatalist*, "have minimal control over their lives. They belong to no groups responsible for the decisions that rule their lives. They are resigned to their fate and see no point in changing it."

It will be interesting to see if these profiles can be found at any organisation, notably in risk management positions. Should a risk manager be of any particular type? Or rather, should he not be of any particular type? Which of the four types is more prone to take a decision (and what type of decision) when facing a specific type of risk?

In this context Douglas and Wildavsky suggest "if some degree of risk is inevitable, suppressing it in one place often merely moves it to another. Shifting risks may be more dangerous than tolerating them, both because those who face new risks may be accustomed to them and because those who no longer face old ones may become more vulnerable when conditions change" (Douglas & Wildavsky, 1992, p. 197).

Beck on the other hand, says "it is the behaviour of others and the behaviour of nature that constitute your risk environment. [...] Human behaviour will always be unpredictable because it will always be responsive to human behaviour. [...] It will never be possible to capture objective risk, however powerful your computer, because the computer's predictions will be used to guide behaviour intended to influence that which is predicted" (Beck, 1992, p. 183).

Risk depends on decisions, Beck concludes, although it requires the right type of personality to take that decision. If so, does it then matter what personality one has – as per Adams' definitions – if it is the others' behaviour that influences ones' risk environment?

As for the four risk assessment methods suggested by Douglas and Wildavsky, they are (Douglas & Wildavsky, 1992, p. 68):

- *revealed preferences* is "based on observation of risks people actually take or accept. Instead of an actual calculation of costs and benefits, it is assumed that [...] these have been internalized and an appropriate balance struck." It is further assumed that in this context individuals have enough information to make conscious choices.
- *expressed preferences* "gets values of the public by asking them". So the big difference is that the previous method restricts itself to passive observation, while this goes actively into the field to gather more information directly from affected

individuals. “Asking people what they would want suggests that this is different from what they are getting”.

- *natural standards* is the method that transfers the burden of decision from the individual to nature, understood as citizenry or society. “Whatever levels of risk man and animals have lived within the past are supposedly tolerable for the future”, mostly because society will take care of it. The problem, the authors say, “is that nature is a mirror reflecting whatever version of reality the looker wishes to see in it. [...] Nature has enough diversity for everyone” so that it can lead to the tacit acceptance of whatever behaviour if no rules and/or guidelines are implemented. The authors give the example of environment protection.
- *cost benefit analysis* is probably the most known method, but for other reasons. In the context of the risk assessment models by Douglas and Wildavsky, “a cost benefit analysis or risk-utility analysis is an effort to compare risks by placing their costs and benefits on a common economic plane.” It might be an interesting thought, but it is highly arguable that all risks can be quantified and measured. The attempts to do quantitative risk management have been highly criticized (see section 2.4 ‘Generic aspects on risk management’).

Current risk management models contain elements of the above methods suggested by Douglas and Wildavsky and each individual can be fit into the profiles as defined by Adams. Later sections will explore details on approaches within the corporate world where these elements can be found. Of course, corporations are managed by individuals which can have certain attributes from the categories suggested by Adams. So it is important to define and understand how an organisation, as combination of various individuals – or as unified group of intrinsically different individuals – faces risk: how risks are identified, valued and mitigated given its own *risk appetite*. This concept will be discussed in the next section.

2.3. Defining risk appetite

As seen above, the perception of risk can vary on the individuals’ age, gender, personality, income, management position and even private circumstances. What is certain on one day, can be questioned the next. If this is true at an individual level, it is more so for a group of individuals managing a company. Therefore generating some sort of objectivity in a room of managers can be a challenging exercise, where the outcome is as volatile as each individual’s risk perception.

Experience gathered by specialised management consultants concluded that “more often than not, a firm’s risk appetite is formed primarily on the basis of managerial instinct” (Oliver Wyman, 2005, p. 2), which is considered to be wrong and potentially a risk by itself due to its inherent volatility and lack of formal judgement.

David Hillson and Ruth Murray-Webster identified in 2007 a number of drivers of corporate risk culture and therefore its risk appetite. They include:

- "The influence of organisational history and corporate memory,
- Recent events having a significant effect on the organisation,
- Reputational issues, past and present,
- Stakeholder expectations and influences,
- The leadership style adopted at all levels in the organisation,
- Characteristics of the industry sector within which the organisation operates,
- The current economic environment and conditions,
- The national and international context for corporate activities."
  (Hillson & Murray-Webster, 2007, p. 29)

In the case of weak leadership, it is easy to fall into the compromise position of 'what is acceptable for all' where everybody has to cede a little, or to proceed to quantification efforts and extract the average of all opinions. Herein resides the difficulty of measurement: not only are some risks unquantifiable, and thus not measurable, but also attempted quantification exercises can have different results, depending on the timing of the exercise or the then predominant mindset (beyond being source for even more confusion and mistakes; see next section). Therefore, averaging – or regression to the mean – is, according to Bernstein's words, "little more than mumbo-jumbo. Never depend on it to come into play without constantly questioning the relevance of the assumptions that support the procedure" (Bernstein, 1996, p. 186). Yet he also states that "gut rules measurement. […]And that's a good thing. If everyone valued risk in precisely the same way, many risk opportunities would be passed up" (Bernstein, 1996, p. 105).

The question to be answered is: 'how can an organisation define what is acceptable?' Or, in other words, 'how much risk is it willing to take?'. This is the basis for the definition of risk appetite. This concept is thus essential for any organisation. It establishes the overall framework for the actual risk management policy to be designed and implemented within the organisation. It defines what an acceptable exposure is by weighing potential losses or rewards. For the purpose of this study, risk appetite will be used as defined in the already cited Guide 73 of ISO 31000:2009.

Figure 13: Definition of Risk appetite

Risk appetite "amount and type of risk that an organisation is prepared to pursue, retain or take"

Source: (International Organisation for Standardisation, 2009c, p. 8)

As will be seen later, other risk standards have slightly different definitions, introducing the terms *value*, *culture* and *operating style*: risk appetite "is the amount of risk, on a broad level, an entity is willing to accept in pursuit of value. It reflects the entity's risk management philosophy, and in turn influences the entity's culture and operating style" (COSO, 2009, p. 3).

David Hillson and Ruth Murray-Webster continue exploring individual risk attitudes and the influences they exert on the organisations perception, behaviour and reaction towards risk. They explore the A-B-C model (attitude influences behaviour, behaviour influences consequences) and reach the conclusion that there are four basic risk attitudes:

- risk-averse,
- risk-tolerant,
- risk-neutral, and
- risk-seeking;

although "the same individual or group may exhibit different risk attitudes under different circumstances" (Hillson & Murray-Webster, 2007, p. 45).

In agreement with this and in line with an individual's risk perception, an organisations' risk appetite "is not necessarily static; in particular the Board will have freedom to vary the amount of risk which it is prepared to take depending on the circumstances at the time" (HM Treasury, 2004, p. 23). It is therefore suggested that not only should the organisation formalise its risk appetite in a written statement, so that it becomes clear for all stakeholders what the organisation is willing to accept and reject, but it should also revisit this regularly as it should become part of the companies' strategic planning process.

According to management consulting firm Oliver Wyman, such a risk appetite statement should include qualitative and quantitative elements, as well as "separate risk into 'acceptable' and 'unacceptable' buckets" (Oliver Wyman, 2005, p. 4). Further on: "unacceptable risks are those that do not help realise the strategic vision" of the company. How such a statement is ultimately formulated – and therefore how the companies' attitude towards risk is defined – depends very much on the companies' own management, leadership style, industry, stakeholders, as well as current and past performance. A very successful company may be less willing to be exposed to specific risks, as a means to protect its market and achieved success (however success is measured). The opposite may also be true.

Quantitative elements can be drawn from tools that are designed to express in value how much risk the company might be incurring in (such as the Value at Risk concepts, applicable to earnings, cash flow, etc.), internal ratios (exposure concentration limits, leverage ratios) or even external sources, such as credit ratings. Qualitative elements refer mostly to compliance level and standard definitions, although they should be aligned with the expectations and requirements of key share- and stakeholders. “If everyone is clear about how much risk the business is prepared to take, it makes it easier to respond swiftly and decisively to market openings and judge where, when and how to expand” (Pandor, et al., 2010).

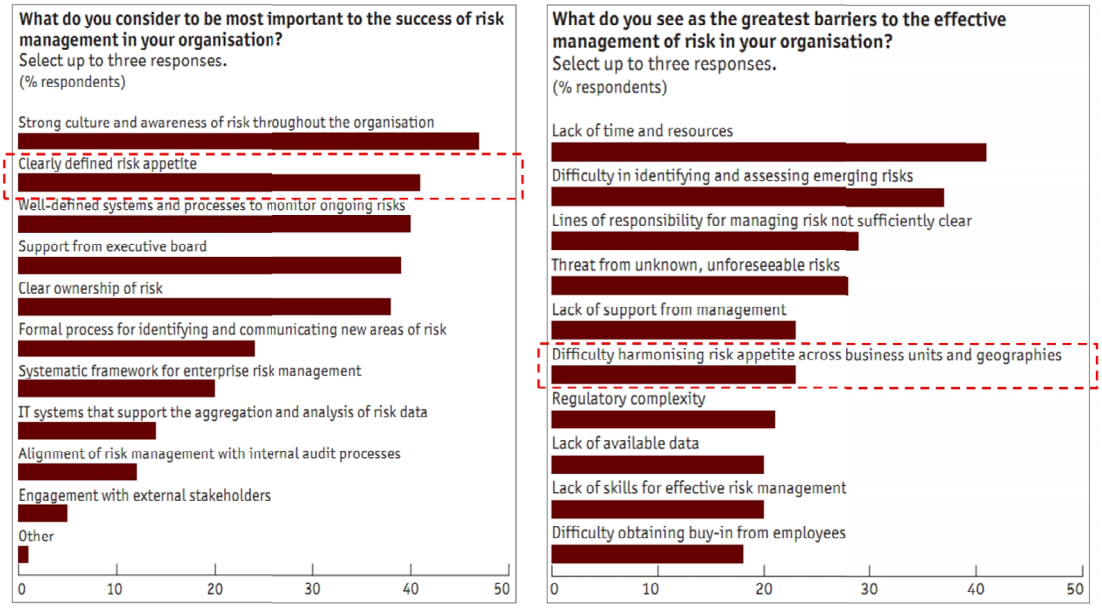
One good example of a clearly defined risk appetite statement is the one of Lufthansa German Airlines, produced in the Annual Report 2011: “Risks count as material if they are capable of causing damage of at least one third of the operating result necessary for maintaining the value of the Company. For 2011 this amount was again determined to be EUR 300m for the Lufthansa Group. The materiality threshold is calculated individually for each of the business segments according to the same principle” (Lufthansa German Airlines, 2012).

This statement contains a metric (*operating result necessary for maintaining the value of the company*), a quantitative threshold (*one third*), its quantification (EUR 300m, for 2011), it is revised periodically and calculated for each business segment. Any risk with calculated impact beyond the threshold will be treated accordingly. As will be seen later, Lufthansa’s risk management organisation is mostly decentralised, thus each business unit is responsible for the management (identification, evaluation, mitigation) of its own risks.

A clearly defined risk appetite has been classified as a key element for companies to successfully manage risks within their organisations (The Economist Intelligence Unit, 2007). In fact, as is visible in the figure below, it is the second most important item just after “strong culture and awareness of risk throughout the organisation”. At the same time, the difficulty of harmonising this risk appetite across all business units and geographies the company has spread into has been seen as a major barrier to introduce effective risk management within the organisation.[3]

[3] These are results of a survey conducted by the Economist Intelligence Unit in 2007 to 218 executives at companies around the world on their approach to risk management.

Figure 14: Risk appetite as key to successfully manage risk



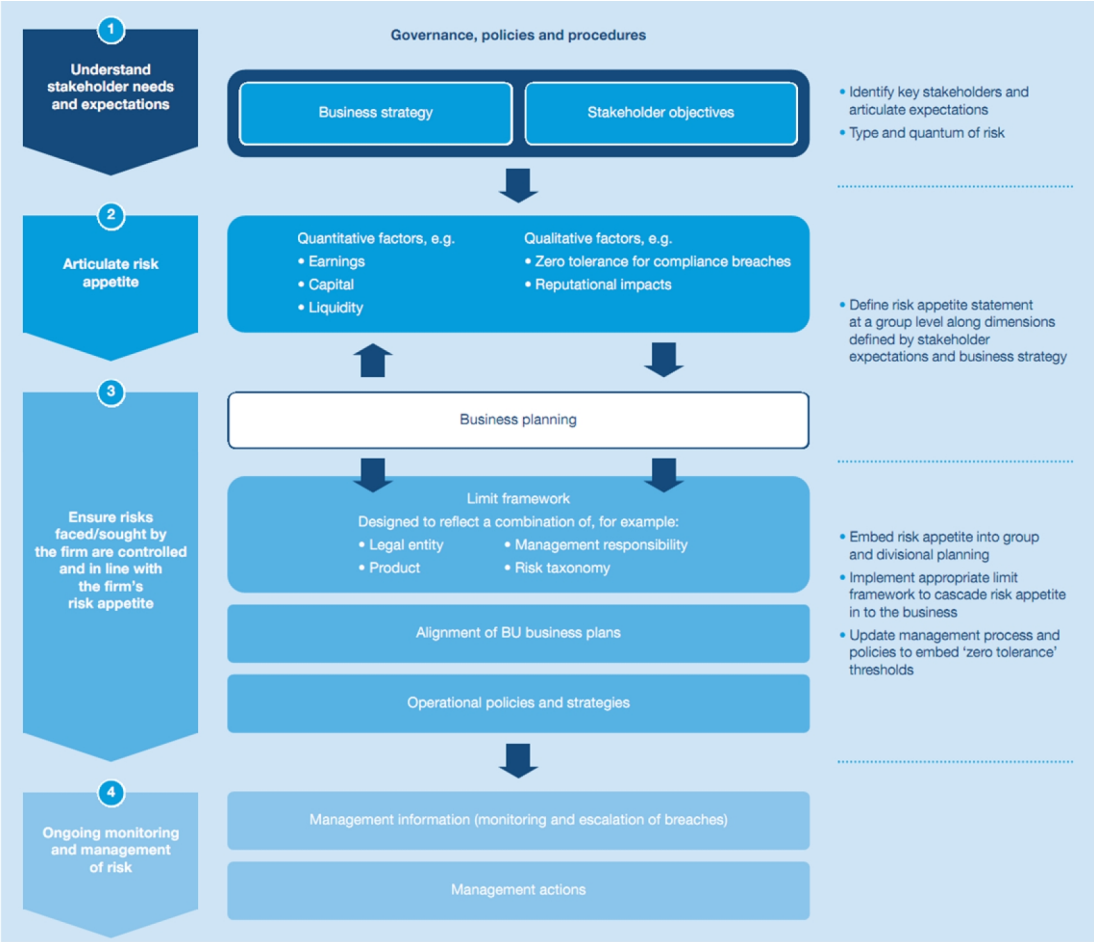
Source: (The Economist Intelligence Unit, 2007, p. 18), own highlights

Interestingly and despite the above, a survey of the National Association of Corporate Directors (a US-based organisation with over 13.000 members in public, private and non-profit companies) cited by Oliver Wyman shows that “70% of board members say their companies have not properly defined their risk appetite” (Pellerin, et al., 2012).

It is thus important to incorporate the correct, complete and accurate definition of a risk appetite statement within an organisation’s internal processes and life. This is visualised in a paper produced by PWC (PriceWaterhouseCoopers, 2010), another management consultancy, where the risk appetite definition process is presented as linked to the overall strategic and business planning process (see below).

In this model the definition of risk appetite is integrated into other corporate definition steps, starting with the understanding of stakeholders’ needs and expectations and how that will influence the overall willingness to and/or acceptance of risk exposure. With further definition steps, risk becomes deeper embedded into the organisation as part of its governance and planning processes enabling a continuous review and monitoring of risk. In this model, Business Planning becomes central to the organisations’ activity providing guidelines for the middle management and quantitative monitoring tools for upper management, although it already embeds and uses the risk appetite defined beforehand.

Figure 15: Risk appetite framework



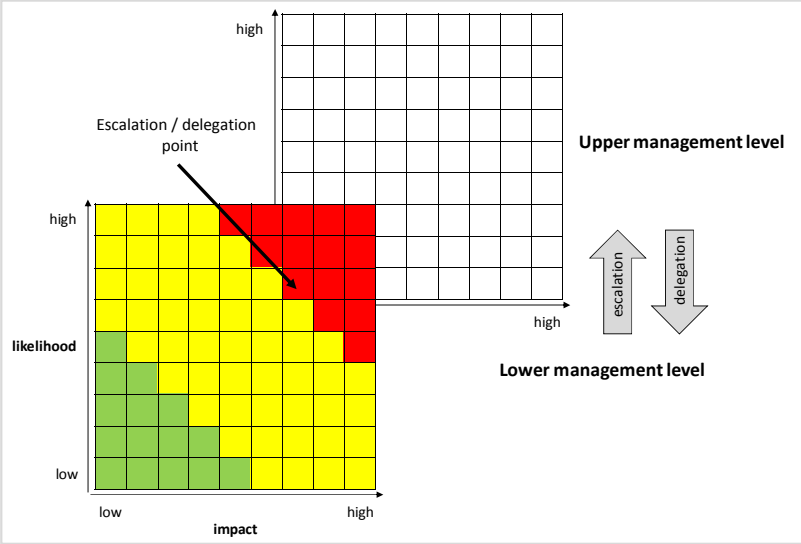
Source: (PriceWaterhouseCoopers, 2010, p. 2)

The Orange Book (by the HM Treasury as quoted earlier) suggests that the corporate risk appetite can be used at intermediate management levels to create layers of risk appetite based on the specific understanding of the function. What is a high risk for an intermediate manager may not be considered as high for upper management and vice versa. Cascading this into the organisation allows for delegation and escalation procedures and therefore better overall risk management by empowering middle managers to act on their specific fields of the business.

Later in this document several risk assessment tools shall be discussed, such as heat maps where each risk can be rated according to its likelihood and impact of happening, from low to high with colour schemes representing the importance of each risk item. In the context of the above cascading risk appetite definition, the heat map layer and escalation process could be depicted as shown in the figure below.

The downside of this approach, beyond definitional and understanding issues associated to the use of a subjective measurement approach, is that such a process may also contribute to the dilution of the perception of a specific risk within the organisation and therefore contribute to not handling that risk item properly.

Figure 16: Delegating and escalating risk appetite



Source: adapted from (HM Treasury, 2004, p. 25)

By applying the risk appetite concept and the respective escalation model, the organisation will automatically have a guidance level for monitoring its own risk management performance and adjust, when and where needed, required resources to achieve its objectives. “If a risk does not correspond to the agreed risk appetite, resources could be focused on bringing it to within the tolerance level. Risks which are already within the agreed tolerance level could be reviewed to see if resources could be moved to more risky areas without negative effects” (HM Treasury, 2004, p. 25).

Nevertheless the applicability of such an escalation and delegation process depends very much on the organisations’ involvement in risk management and its resource availability. Certainly, smaller organisations have a much better overview and quicker decision making process than larger organisations, therefore not requiring elaborate models.

The biggest requirement in this concept is the mobilisation of the entire organisation around the importance of risk. Without proper acknowledgement of the risk management process, no delegation (and escalation) can work. The next sections will first discuss generic aspects on risk management itself and then typical reasons for failure of risk management processes.

2.4. Generic aspects on risk management

As mentioned before, every person (at an individual level and regardless of their values of beliefs, nationality or origin) as well as every organisation (regardless of their size and ownership) are exposed to risks of various natures and origins. Depending on the person's or organisations' willingness to accept risk – ultimately their risk appetite – they may be exposed to hundreds of items that can be classified as risk. Managing all of them is impossible, not only due to the large number, but also due to the natural limitation of resources (human, technical, financial, etc.) every person and organisation sooner or later have to face.

This section will therefore explore what currently available literature presents on some aspects on risk management, notably on:

- defining risk management as a process,
- presenting a way to identifing an organisations' risk maturity,
- describing types and sources of risk,
- describing commonly used techniques to identifying risks,
- presenting typical risk treatment options, and
- addressing organisational aspects.

2.4.1. Defining risk management as a process

Douglas and Wildavsky state: "if the selection of risk is a matter of social organisation, the management of risk is an organisational problem. Since we do not know what risks we incur, our responsibility is to create resilience in our institutions. But by choosing resilience, which depends on some degree of trust in institutions, we betray our bias toward the centre." (Douglas & Wildavsky, 1992, p. 198). This statement leads to the discussion of what risk management is and how it can be organised. It also emphasizes the importance of resilience, another element that should be well understood by all organisations.

As defined by ISO, resilience is the "adaptive capacity of an organisation in a complex and changing environment" (International Organisation for Standardisation, 2009c, p. 11); without this capacity organisations become weak and vulnerable to all those internal and external shocks. Improving resilience, setting the ground for sustained development and long-term survival is a responsibility that each manager should have. Nevertheless, one should not forget that organisations and respective decision makers are people that have

their own opinions, beliefs and values, and thus influence the overall attitude the organisation will have towards specific items.

It is difficult to judge how resilient an organisation can become; it is a very unquantifiable statement as any event can always endanger its existence and put established processes to a test. Therefore, following Adams' suggestions, one can ask 'how can we manage risk better'? (Adams, 1995, p. 208). Recalling the four personality features Adams identified in his studies, each could have different attitudes:

- "the *fatalist* will answer 'no, we cannot manage risk better; life is unpredictable and that is the end of it'";
- "the *individualist* will be of the opinion that there should be a devolution of managerial responsibility from bureaucracy to the individual";
- "the *egalitarian* will favour the exercise of more caution and cooperation";
- "the *hierarchist* will advocate more research and regulation".

No agreement will and could ever be achieved, Adams suggests, as it would halt reaping the benefits of multiple perspectives over events. We cannot all have the same opinions: "if we were all fatalists, life would be nasty, brutish and short" (Adams, 1995, p. 208).

Therefore, within an organisation the best way to manage risk is to combine all perspectives and formalise management efforts into a well defined process. At an earlier stage, risk management has been defined as "coordinated activities to direct and control an organisation with regard to risk" (International Organisation for Standardisation, 2009c, p. 2). Relevant terms are *coordinated*, *direct* and *control*.

Risk management should be *coordinated* so that the entire organisation moves into the same direction. If every unit has its own attitude towards risk, and adopts conflicting actions to face one event, the organisation will certainly suffer at operational, financial and strategic levels. Thus, by harmonising actions it will be possible to steer – or *direct* – the organisation towards the achievement of its predefined goals. And by identifying risks and adopting coordinated actions, it will be easier for the organisation to monitor – or *control* – its overall performance, mitigation strategies or contingency plans necessary to cope with those risks. Again: "the management of risk is an organisational problem" (Douglas & Wildavsky, 1992, p. 198). And as it happens most of the times, organisational problems can be solved by introducing a process (that should be well defined, communicated and implemented) mobilising the entire organisation towards solving that problem. In this case it will be a *risk management process*.

Figure 17: Definition of risk management process

Risk management process "systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk"

Source: (International Organisation for Standardisation, 2009c, p. 3)

A risk management process as defined by the International Organisation for Standardisation will help, because:

- It is systematic, therefore repetitive, revolving and consistent;
- It involves policies, procedures and practices that have been designed with the sole purpose of managing the company, its operations, internal and external environment, etc. thus as many sources of risk as possible.
- It defines seven clear steps, clearly showing how such a process could (or should) be visually depicted:
    1. communication and consultation,
    2. establishing the context,
    3. risk identification,
    4. risk analysis,
    5. risk evaluation ,
    6. risk treatment,
    7. monitoring and review.

ISO's risk management model will be further explored in a later chapter. What is relevant at this stage is to stress that risk management should be a process with clearly defined steps. Yet before jumping into the implementation of such a model, any organisation should understand the concept of risk, its own risk attitude (as defined above) and carefully prepare itself and understand how mature it is towards risk.

2.4.2. Identifying an organisations' risk maturity

Several authors suggest an organisation should start by assessing the maturity of its current processes and positioning towards risk and risk management. It is safe to say that organisations with no risk management processes in place are not 'risk mature': identification, assessment and mitigation are probably done informally and on a case-by-case basis, with no formal and consistently implemented procedures throughout its business existence. Nevertheless, the opposite is not necessarily true. Organisations that have done some efforts in the field of risk management, by producing lengthy process descriptions for risk identification and evaluation or even implementing some mitigation measures, are not immediately 'risk mature'. The way organisations embed and absorb

these processes is key: if individuals are aware of possible risks, know the rules and proceed naturally, even if an event occurs, then it is likely that they are managing risk properly.

Baxter cites a risk maturity model developed by De-RISK, a specialised risk management consultancy, based on the *capability-maturity-model-integration* (CMMI) initially developed in the late 1980s for IT software development projects and then adapted for risk management purposes (Baxter, 2010, p. 191). This matrix enables the identification of an organisations' positioning towards risk management using a standard set of parameters in five different categories. Of course, if an organisation needs a more granulated approach it can expand these categories into those it feels necessary (e.g. operations, finance, etc.).

The five categories are:

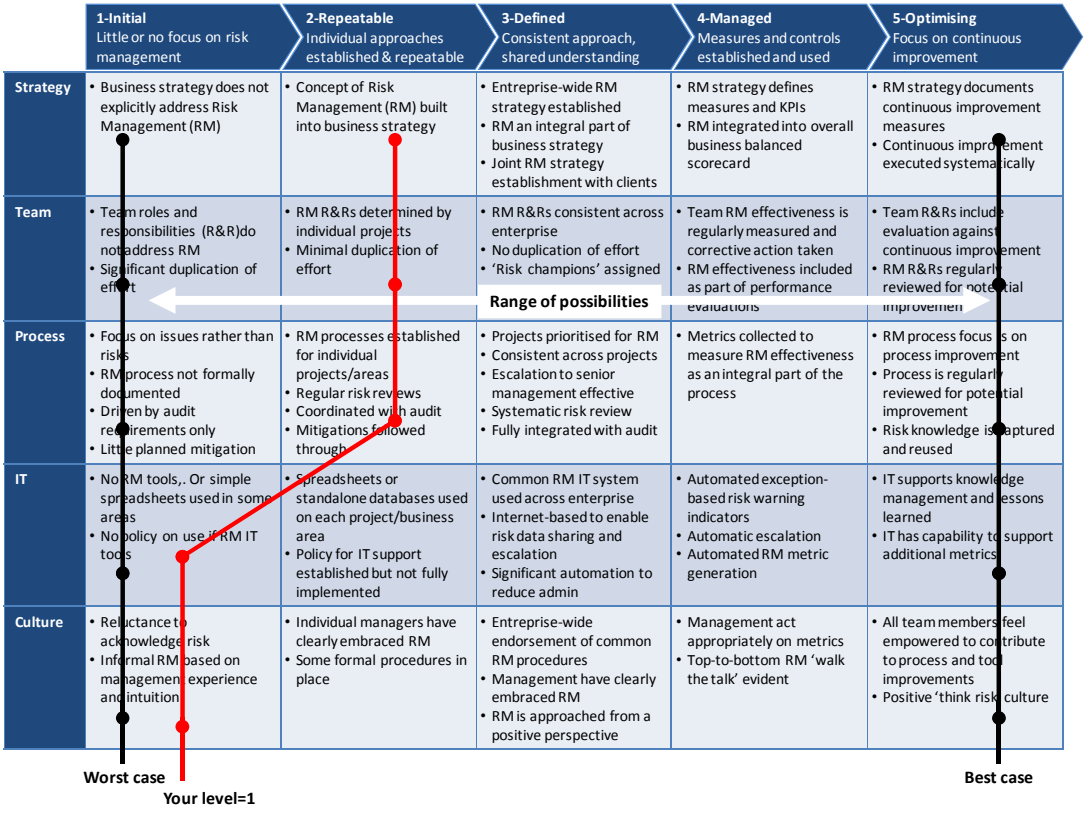
- Strategy, highlighting how the current corporate strategy incorporates risk management practices. It ranges from inexistent risk management to full integration of risk management into strategy documents.
- Team, addressing roles and responsibilities of risk management within the existing structures and workforce. An organisation that has unclear task and responsibility definitions will not be as well off as an organisation that has clear allocation of responsibilities for risk management (the 'risk champion').
- Process, covering the formalisation of risk management within the organisation: from no or only loosely defined processes to a fully documented and process focused approach.
- IT, in order to understand if the organisation uses no or rudimentary tools to document, register and monitor risks or if there is a more sophisticated tool-based approach that enables automatic early warnings and monitoring.
- Culture, trying to understand if the organisation has a negative predisposition towards risk (and is thus risk averse) or if there is a more positive culture in place, viewing risk as a positive element that might lead to business expansion and development.

The two figures below depict the risk maturity matrix and the ranges of ranking options. Positioning an organisation in these categories 'only' requires identifying what statements best describe the current status-quo. The ranking starts at the 'Initial' level where there is no focus on risk management and go up to 'Optimising' where there are well developed risk management processes and these are fully integrated into corporate strategy and culture. Baxter suggests that an organisation should always adopt, as global score, the lowest level it achieved in any category. "The idea is that you are only as good as your weaknesses" (Baxter, 2010, p. 192).

Figure 18: Risk management maturity matrix (based on CMMI)

	1-Initial Little or no focus on risk management	2-Repeatable Individual approaches established & repeatable	3-Defined Consistent approach, shared understanding	4-Managed Measures and controls established and used	5-Optimising Focus on continuous improvement
Strategy	• Business strategy does not explicitly address Risk Management (RM)	• Concept of Risk Management (RM) built into business strategy	• Entreprise-wide RM strategy established • RM an integral part of business strategy • Joint RM strategy establishment with clients	• RM strategy defines measures and KPIs • RM integrated into overall business balanced scorecard	• RM strategy documents continuous improvement measures • Continuous improvement executed systematically
Team	• Team roles and responsibilities (R&R)do not address RM • Significant duplication of effort	• RM R&Rs determined by individual projects • Minimal duplication of effort	• RM R&Rs consistent across enterprise • No duplication of effort • 'Risk champions' assigned	• Team RM effectiveness is regularly measured and corrective action taken • RM effectiveness included as part of performance evaluations	• Team R&Rs include evaluation against continuous improvement • RM R&Rs regularly reviewed for potential improvement
Process	• Focus on issues rather than risks • RM process not formally documented • Driven by audit requirements only • Little planned mitigation	• RM processes established for individual projects/areas • Regular risk reviews • Coordinated with audit • Mitigations followed through	• Projects prioritised for RM • Consistent across projects • Escalation to senior management effective • Systematic risk review • Fully integrated with audit	• Metrics collected to measure RM effectiveness as an integral part of the process	• RM process focus is on process improvement • Process is regularly reviewed for potential improvement • Risk knowledge is captured and reused
IT	• No RM tools,. Or simple spreadsheets used in some areas • No policy on use if RM IT tools	• Spreadsheets or standalone databases used on each project/business area • Policy for IT support established but not fully implemented	• Common RM IT system used across enterprise • Internet-based to enable risk data sharing and escalation • Significant automation to reduce admin	• Automated exception-based risk warning indicators • Automatic escalation • Automated RM metric generation	• IT supports knowledge management and lessons learned • IT has capability to support additional metrics
Culture	• Reluctance to acknowledge risk • Informal RM based on management experience and intuition	• Individual managers have clearly embraced RM • Some formal procedures in place	• Entreprise-wide endorsement of common RM procedures • Management have clearly embraced RM • RM is approached from a positive perspective	• Management act appropriately on metrics • Top-to-bottom RM 'walk the talk' evident	• All team members feel empowered to contribute to process and tool improvements • Positive 'think risk' culture

Figure 19: Risk management maturity matrix (based on CMMI, example)



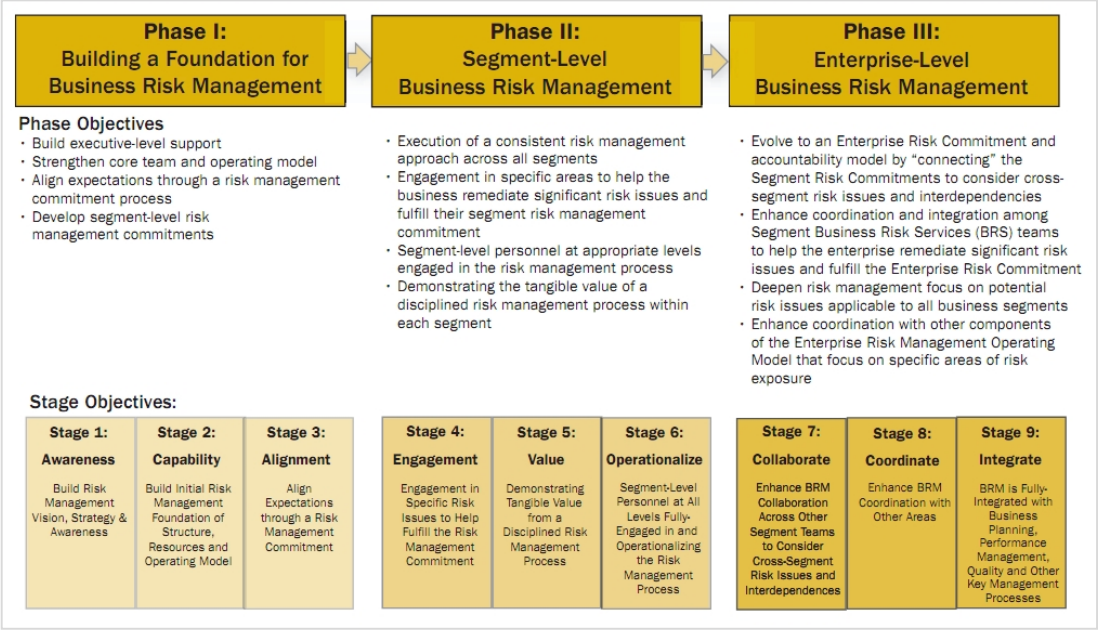
Source: (Baxter, 2010, p. 193)

Baxter says “most organisations will start this process by assessing themselves to be at level 1 and few will start at level 2. Personally, I have never come across an organisation that is at level 3 on their first assessment” (Baxter, 2010, p. 192). This indicates that multiple and regular assessments should be done over time.

Therefore, this model helps tracking improvements made by an organisation that has started to implement risk management processes. In this case, the ideal tendency would be to see a movement rightwards in the matrix, showing an increased awareness and integration of risk-related items in the organisation, making it more ‘mature’ in this sense. If there is a leftward movement, then corrective actions need to be put in place.

On the same risk maturity topic, the Institute of Management Accountants (IMA), a US-based professional entity representing management accountants, suggest another type of model for risk maturity assessment, after a risk management process has been implemented. This is a phased model, structured in 3 distinct and subsequent phases, each representing deeper integration of risk management within the organisation.

Figure 20: Risk management maturity model (based on IMA)



Source: (IMA, 2007, p. 24)

In this model, each phase is divided into three stages, each representing specific actions to be implemented in order to increase risk maturity within the organisation. Phase 1 focuses on gathering the basics, such as building risk awareness, capabilities, identify and align expectations on risk management outcomes within the organisation. Phase 2 intends to

involve staff within each business segment, engaging them in the implementation and daily execution of risk management activities, demonstrating value from the process. Phase 3 connects risk management efforts of each business segment, solving cross-segment issues and interdependencies. It is expected that by Stage 9 (Integrate, in Phase 3) the organisation is at its highest level of risk maturity and therefore dominates all relevant risk management techniques.

While this model outlines individual steps to implement a risk management process to achieve a more mature state, the CMMI adaptation shown above enables a more rigorous evaluation of status quo and evolution towards the desired state. Associating targets and deadlines transforms this model into a powerful tool to track risk maturity within the organisation. In this context, it is also relevant to address the importance of the Board of Directors in the whole process of risk management implementation and maturity tracking[4].

Brodeur and Pritsch, at McKinsey, produced a report fully dedicated to "Making risk management a value-adding function in the boardroom", and therein present some ideas on how a board can and should be involved in a risk management process.

Figure 21: Sample board self-assessment questionnaire

Board self-assessment example

A. Oversight – how well does the board understand…	Not at all 1	2	3	4	Completely 5
• The major risks the company faces?	☐	☐	☐	☐	☐
• Alignment of the current risk profile with its risk strategy?	☐	☐	☐	☐	☐
• The risk-return tradeoffs and the risk-adjusted level of value creation of each line of business?	☐	☐	☐	☐	☐
• Any new types of risk assumed as well as material, extraordinary transactions (e.g., acquisitions of low portfolio, off-balance-sheet transactions)?	☐	☐	☐	☐	☐
• Structure and effectiveness of risk management infrastructure at both corporate and BU levels?	☐	☐	☐	☐	☐
• Philosophy, structure, and effectiveness of corporate risk policies?	☐	☐	☐	☐	☐
• Potential conflicts between risk strategy and policies and compensation systems?	☐	☐	☐	☐	☐
• Progress made against commitments made to board?	☐	☐	☐	☐	☐
B. Effectiveness of committee structure					
• Are the committee charters and responsibilities appropriate and shared by all members?	☐	☐	☐	☐	☐
• Is the committee composition adequate?	☐	☐	☐	☐	☐
C. Effectiveness of board meetings					
• Do the board meetings focus on the core issues (as opposed to, for example, the tactical review of nonmaterial transactions)?	☐	☐	☐	☐	☐
• Do all committee members have an adequate understanding of risk management issues?	☐	☐	☐	☐	☐
• Do all committee members contribute productively to the discussion?	☐	☐	☐	☐	☐
• Is the meeting frequency appropriate?	☐	☐	☐	☐	☐
• Do all committee members attend and prepare for board meetings adequately?	☐	☐	☐	☐	☐
• Is the material presented in a way that enables the committees to fully understand critical issues and decision needs?	☐	☐	☐	☐	☐
• Are the discussion materials for the meetings distributed in advance?	☐	☐	☐	☐	☐

Source: (Brodeur & Pritsch, 2008, p. 13)

[4] Organisational issues will be addressed in a separate section of this document.

What is relevant for the present risk maturity discussion is a questionnaire proposed by these authors to gather the Boards' understanding on internal risk management issues. This of course is the result of a wider effort and opens the doors to other issues, such as corporate governance, management independence, communication flows and decision making processes, which are not object of this study.

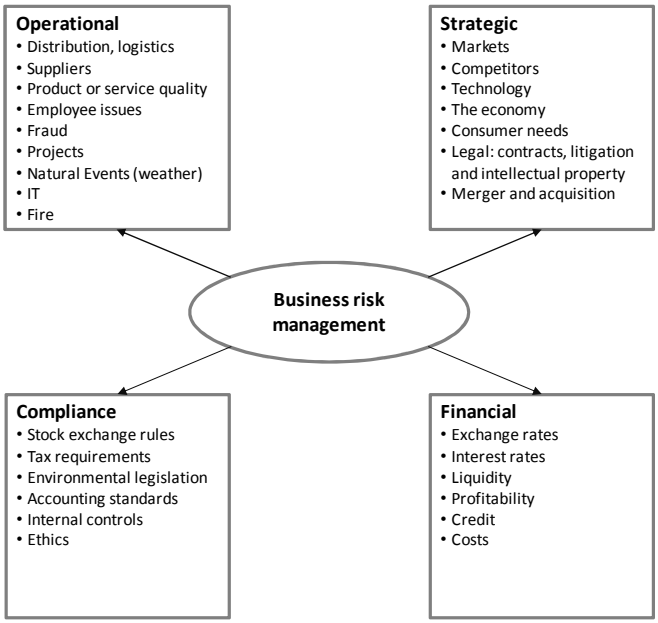
With such a questionnaire, perhaps enlarged to cover more strategic issues, it might be possible to involve the Board for the need to have an effective risk management process in place and thus allocate resources for its proper design and implementation. If the average results of this questionnaire, when applied to all Board members, are between 1 and 2, one can immediately see that the risk management topic is not placed very high on the Boards' agenda. The repeated application and response tracking over time helps, as seen in the CMMI model above, the evolution of the perception and understanding of risk management - in this case at Board level. Of course, similar questionnaires can be applied to any management level to capture their opinions on the subject.

2.4.3. Types and sources of risk

The number of possible risks is endless and these keep increasing with the enlargement of an organisations' activities (commercial or not). So do the sources of risk, becoming more voluminous and diversified with the increasing complexity of business transactions and other sorts of interactions between entities. As for sources, these can be of internal or external origin, either being purely related to the organisation or involved stakeholders. To shed some light into all these possibilities, some authors have grouped all possible risks (Sadgrove, 2005, p. 18) and (IMA, 2007, p. 5):

- Operational risks, representing all those directly related to the main activities of the organisation (in the case of an airline this would be providing air transport services for passengers and cargo), regardless of being of internal nature (e.g. production processes) or external (e.g. supply chain issues).
- Strategic risks that are directly linked to the strategic management of the company, thus emanating from decisions coming from upper levels of the management hierarchy (e.g. own and competitors' growth projections, investment decisions, merger and acquisition plans, etc). Not identifying and mitigating them on-time can lead to disastrous consequences for the organisation, putting its survival at stake.
- Compliance risks, relate to all those issues that are formally regulated by state authorities, industry bodies, para-national entities, etc., all particularly significant for airlines. Examples are EASA, FAA or ICAO regulations that must be adhered to.
- Financial risks are self explanatory and can have internal and external origin.

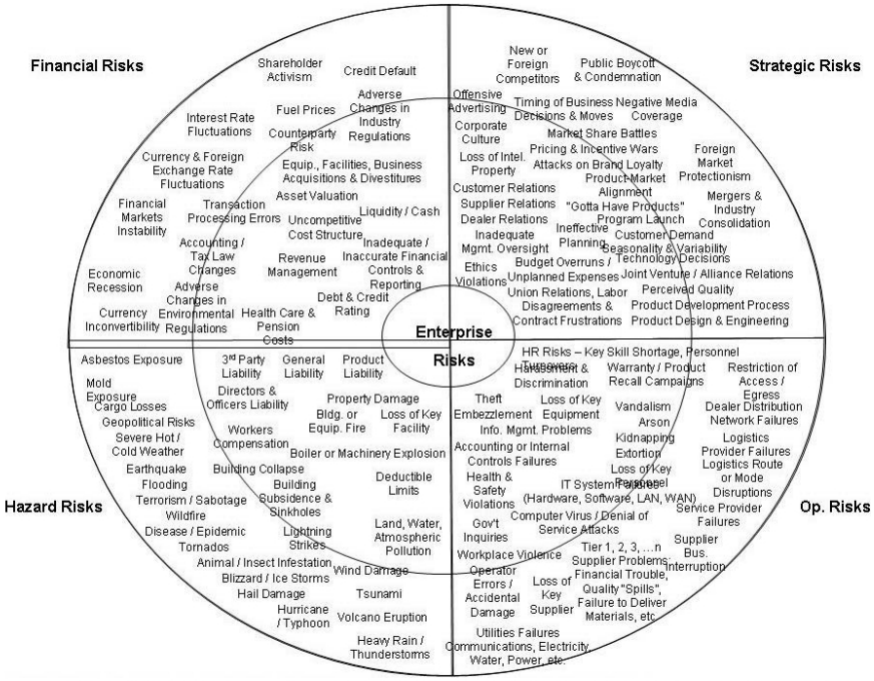
Figure 22: Four types of risk



Source: (Sadgrove, 2005, p. 20)

The IMA report cited earlier shows a depiction of a risk landscape for an industry portfolio, citing another author (Debra Elkins), using these four categories. The number and diversity of items make this depiction almost illegible, despite all simplification efforts.

Figure 23: Industry portfolio of risks



Source: Debra Elkins, "Managing Enterprise Risks in Global Automatic Manufacturing Operations," presentation at the University of Virginia, January 23, 2006. Permmission granted for use.

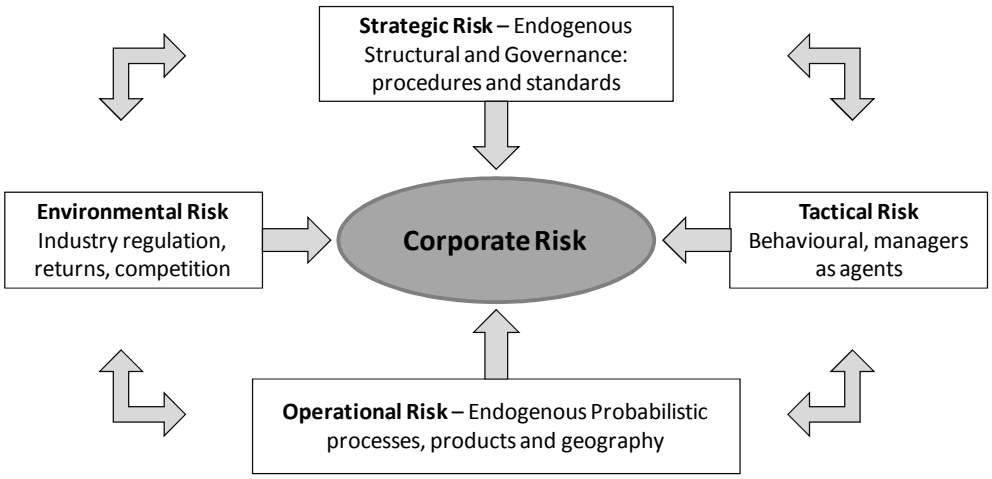
Source: (IMA, 2007, p. 5)

Buehler and Pritsch at McKinsey present slightly different categories (Buehler & Pritsch, 2003, p. 3):

- Market risks, refer to "adverse price movements" of raw materials, end products or even financial securitisation tools, exchange rates, interest rates and spreads.
- Credit risks, relate to all instances when an organisation is not able to meet its financial obligations and thus enters into default with its creditors. The recent Euro-zone crisis was mostly a credit risk crisis, as some countries in Europe were not able to comply with payments to be made as bonds issued achieved their maturity.
- Operational risks, as above, relate to all those events that can arise from the day-to-day business activities of the organisation.
- Business-volume risks, are those "stemming from changes in demand or supply or from competition, exposing its revenue volatility".

In yet another form and naming, Coleman presents 4 sources of corporate risk: strategic risk, tactical risk, operational risk and environmental risk, putting emphasis on the internal human element in the tactical risks and the external and possibly uncontrollable elements in the environmental risks. In this model, risks of each source influence risks of other sources, exposing inherent interrelationships and interdependencies.

Figure 24: Sources of firm risk



Source: (Coleman, 2009, p. 16)

Coleman also stresses the endogenous character of strategic and operational risks. "For instance, Rumelt analysed risk or uncertainty in US company profits as measured by their variance and found that around half was explained by firm-specific factors (and only 16 per cent by industry-specific factors). The endogenous nature of firm risk was confirmed by Palmer and Wiseman who found that at least 20 per cent of organisational risk propensity

is explained by managers' risk attitudes, and relatively little by external factors such as industry structure" (Coleman, 2009, p. 16).

It is debatable if this should lead to the exclusion of the external element in risk source identification. In some industries (notably air transport), even if internal decisions and management style might be source for a large portion of risks, external elements carry a heavy weight and are conditioning daily decision making. It might therefore not be the best way to approach risk identification, as some sources are excluded from the analysis.

While the above models are typically used in industry-neutral environments, each organisation should be able to categorise risks according to its own needs and requirements, very much depending on the industry it is working in and the attitude the organisation has towards risk itself.

Aerosafe, an Australia and New Zealand based risk management consultancy specialised in aviation, produces a different categorisation, using three categories distinguishing hazard from risk and considering each risk as a possible source for opportunities (Aerosafe, 2012):

- Uncertainty-based risks
- Opportunity-based risks
- Hazard-based risks

These aviation-specific definition and interpretations shall be addressed in later chapters.

2.4.4. Risk identification techniques

Identifying risks is probably one of the most important steps in the entire risk assessment and risk management process. The risk assessment process (according to ISO 31000:2009, the most recent standard, and used as guiding reference throughout this study) is composed of three steps: risk identification, risk analysis and risk evaluation. Without proper identification, no risk can be properly evaluated, mitigated and monitored – especially and by definition, unidentified ones. Of course, not everything can be a risk: a specific item or event 'must' be powerful enough to endanger the successful achievement of an organisation's goals. Recalling the definition presented earlier, a risk is "the effect of uncertainty on objectives" and uncertainty is clarified as being "the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood" (International Organisation for Standardisation, 2009c, p. 1).

Therefore, more than managing a risk by itself, the risk management process aims at managing the consequences a particular event might have. Managing a volcano eruption, an earthquake, or the aforementioned forest fires is impossible; what organisations can do is to manage *effects* of these events on their own business. Key assumption is thus that the respective event has been properly identified. Yet, Kevin W. Knight, Chair of the International Organisation for Standardization, referring to the Icelandic volcano eruption in April 2010, wrote: "surprisingly such an event does not appear to have featured as a risk that airlines and many other companies needed to manage…Given knowledge of the activity of the Icelandic volcano and the impact on aviation of past eruptions in Asia, it is surprising that no plans were in place to manage such a disruption-related risk." (Knight, 2010).

When identifying risks, having the organisations' overall objective in mind is essential in order to help classifying an item as a risk or not and properly describing it. The Orange Book presents some simple examples depicted below.

Figure 25: Risk identification vs objective setting

Objective – to travel by train from A to B for a meeting at a certain time	
Failure to get from A to B on time for the meeting	X this is simply the converse of the objective
Being late and missing the meeting	X This is a statement of the impact of the risk, not the risk itself
There is no buffet on the train so I get hungry	X this does not impact on achievement of the objective
Missing the train causes me to be late and miss the meeting	✔ This is a risk which can be controlled by making sure I allow plenty of time to get to the station
Severe weather prevents the train from running and me from getting to the meeting	✔ This is a risk which I cannot control, but against which I can make a contingency plan

Source: (HM Treasury, 2004)

So the question is: how can organisations properly identify risks?

The Institute of Management Accountants presented a quite exhaustive list of possible tools and techniques that may help organisations identifying risks (IMA, 2007, p. 4). Other sources present similar tools (COSO, 2004). Some are also used in other management processes, yet their input can be valuable for risk identification purposes, too. They include:

- Brainstorming sessions
  This implies involving business unit specific or internal cross-functional staff to freely debate issues that may impact the organisation. This exercise helps gathering different opinions and viewpoints, while also serving as means to think out of the

box and of not-so-common items. Having clear rules on the purpose and conduction of the workshop (such as freedom of speech, full respect of opinions or no obedience to functional hierarchies) is essential to produce a fruitful discussion.

- Event inventories and loss event data
  Gathering information on and/or keeping a database of past events that impacted the organisation, the industry it is working in or even the wider geographical economy where it operates, and respective mitigation strategies adopted by the organisation at the time of their occurrence, might constitute a helpful means to manage future events.
- Interviews and self assessment
  Involving internal and external subject matter experts in gathering intelligence and opinions about past and future events is another helpful risk identification method. Performing self assessments – in line with what was presented above, using questionnaires or standardized models – helps positioning the company in its environment, regarding aspects such as market, competition, production methods, human resources, financial performance, etc. Benchmarking exercises are very popular, too, although they must rely on available information – thus on historic evidence (and the past may not be enough to foresee future events and performances – see a later section on 'Why traditional risk management fails').
- Facilitated workshops
  Inviting an external facilitator, familiar with workshop techniques geared towards achieving the most of such gatherings, or using automatic voting software as by the IMA "allows individuals to identify and rank anonymously without fear of reprisal should their superior be a member of the group" (IMA, 2007, p. 7).
- SWOT analysis
  This is a very popular tool for strategy development, as it enables a thorough scanning of internal (Strengths and Weaknesses) and external elements (Opportunities and Threats) surrounding the organisation. The IMA suggests that "for SWOT to be effective in risk identification, the appropriate time and effort must be spent on thinking seriously about the organisation's weaknesses and threats". In the same line of the SWOT analysis, another popular tool is the PESTEL analysis, focussing on political, economic, social, technological, environmental and legal issues. More than internal conditions, the PESTEL analysis focuses on specific categories surrounding the organisation. It might be adapted to the organisations needs, enlarging or shortening the number of categories listed.
- Risk questionnaires and risk surveys
  Performing these regularly enables an organisation to track the development of risk perception and internal awareness on the subject. It is also an anonymous way to collect information even from lower ranked staff, traditionally not heard or invited into brainstorming sessions or facilitated workshops.
- Scenario analysis
  "What if...?" and answering these questions with the best available knowledge is a great way to think outside the box. This helps identifying shortcomings of the organisation and design plans to mitigate the consequences of those events.

Recalling the volcano example mentioned earlier: many volcanoes have erupted before in other geographies and some had impacts on the local air transport industry. What happened to the European aviation industry was a simple lack of scenario planning: answering the simple question "what if a volcano erupted in Europe affecting our regular operations?" could have helped solving the problem.

- Using technology
  Over the recent years a number of IT-based tools have been developed, capable of analysing and computing algorithms capturing the always increasing complexity. While these serve mostly risk analysis and evaluation steps, they can also act as early warning systems. Yet, as in other cases, these tools rely on historical data that may not present valuable information for future purposes. Data quality aspects should also not be forgotten, as attempt to avoid the 'Garbage In, Garbage Out'.
- Other techniques
  Such as decision trees, influence diagrams, value chain analysis, supply chain analysis, process mapping or the aforementioned best practice or peer benchmarking can be valuable, too.

2.4.5. Risk analysis and evaluation aspects

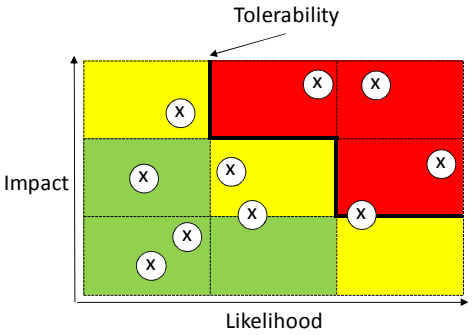
Literature suggests a number of different quantitative and qualitative risk analysis and evaluation methods that help prioritising, create visibility and focus on the most important ones. A reference document published by the Committee of Sponsoring Organisations of the Treadway Commission even suggests templates for each of the individual analysis techniques (COSO, 2004). This section is therefore not going to address them in detail, just discussing in a high level what the most relevant aspects are.

The simplest (perhaps even simplistic) way to evaluate any risk is to classify their likelihood and impact in a scale of 1 to 5 (or 1 to 4 to avoid the 'falling in the middle' trap), from low to high, according to the knowledge and judgement available at the day of the evaluation. While being basic, it is already a step towards the right direction as some organisations are not even using this. Displaying all risks graphically helps create visibility and eliminate items that are not within the predefined appetite levels.

The Orange Book suggests a template on this risk matrix, also displaying the limit of tolerability. This limit is set by each organisation depending on its own strategy and attitude towards risk. Another depiction (Coleman, 2009, p. 96) suggests possible actions to individual risks placed in specific quadrants of that matrix. If a risk has low probability and low impact on the organisation (low consequences), then it is suggested to control and monitor its development. If an item has a high impact on the organisation and it has a high

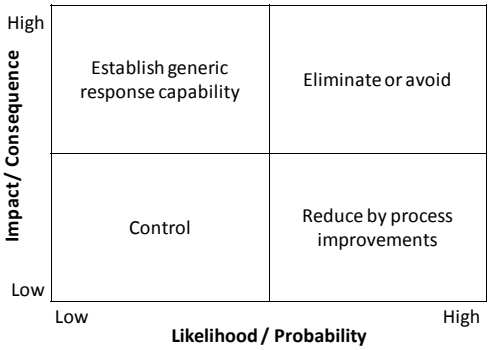
likelihood of happening, then it is suggested to eliminate or avoid that risk. Risk treatment options will be addressed in the next section.

Figure 26: Risk tolerability matrix



Source: (HM Treasury, 2004, p. 19)

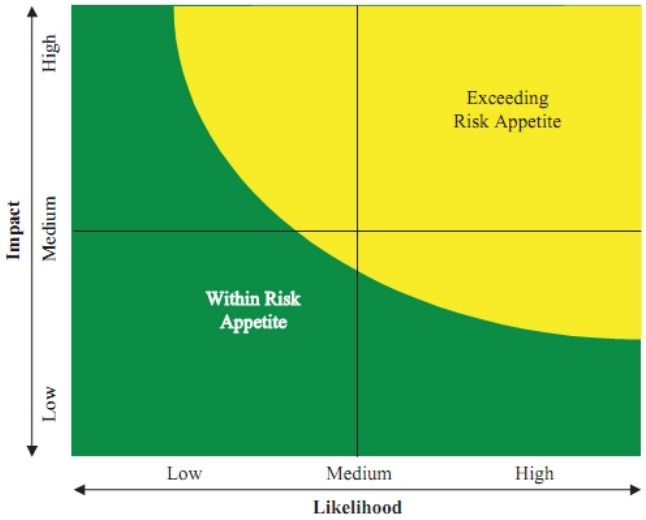
Figure 27: Risk map



Source: (Coleman, 2009, p. 96)

COSO takes this risk map approach a step further and combines it with the organisations' risk appetite (although this is used in the context of addressing residual risk – a topic that will be addressed in the next section). All items within the 'green zone' are considered acceptable; for all items falling within the 'yellow zone' management should adopt actions to reduce the probability of that item having a negative impact on the organisation.

Figure 28: Risk map and risk appetite



Source: (COSO, 2004, p. 17)

Further analysis methods include qualitative and quantitative methods, as well as methods involving a mix of both characteristics. The IMA presents a summary of these methods,

ranging from the above mentioned risk maps to more complex probabilistic analysis methods that apply statistical techniques.

Figure 29: Quantitative and qualitative risk evaluation methods

Source: (IMA, 2007, p. 12)

One example of an analysis method that combines quantitative and qualitative elements is a *heat map*, as presented by Buehler and Pritsch, where the colours represent the gravity of the respective item. This is another visual depiction of the same statements: items with a higher quantitative result get a qualitative classification associated to it.

Figure 30: Heat map

A heat-seeking approach

Annualized earnings at risk for disguised global financial-services company, $ million

Risk concentration
High (>10% of capital)
Medium (>5% of capital)

	Business unit							
	A	B	C	D	E	F	Other	Total
Total market risk[1]	55	**275**	25	10	15	5	10	395
Credit risk[2]	**150**	**350**	**125**	**625**	40	N/A	N/A	1,290
Operational risk	30	**210**	30	**150**	10	2	N/A	432
Business-volume risk	80	**270**	60	**275**	25	5	5	720
Total earnings at risk	315	1,105	240	1,060	90	12	15	2,837

[1]Includes equity-market and interest-rate risks.
[2]Includes lending, investment, and counterparty risks.

Source: (Buehler & Pritsch, 2003, p. 46)

More quantitative methods, such as probability distributions, Value at Risk models or others mentioned above imply the availability of a broad statistical database sufficient in size and quality to make statistical inferences. When this is not the case, some if not all quantitative methods become useless. This study will not focus on individual risk analysis methods (section 'Why traditional risk management fails' will explain why).

2.4.6. Risk treatment options

After having analysed and evaluated the identified risks, the next step is to act upon them. Ignoring their existence is not a solution. Literature suggests various risk treatment options that will be cited below. An organisation may chose to adopt one option depending on the specific risk, its nature and impact, the resources required to mitigate it and the costs associated to that treatment strategy.

The Orange Book refers to five treatment options (HM Treasury, 2004, p. 27):

- Tolerate, when the organisation consciously chooses to accept a risk, without implementing any mitigation measures. A contingency plan might be developed in case the event occurs, yet no further investment is made. A paper produced on Risk Management Policy and Framework (Government of South Australia, Department of Health, March, 2006) describes this as *risk acceptance,* where "the organisation takes a calculated risk and knowingly assumes responsibility for the consequences".
- Treat, when the organisation takes measures to control or reduce the exposure to that risk. There are four types of controls:
    - Preventive controls, "designed to limit the possibility of an undesired outcome", such as separation of responsibilities, internal process auditing and detailed job descriptions.
    - Corrective controls, "designed to correct undesirable outcomes" of events that have already happened.
    - Directive controls, "designed to ensure that a particular outcome is achieved", such as guidelines, plans and policies specifying steps that guarantee the achievement of desired results.
    - Detective controls, "designed to identify occasions of undesirable outcomes having been realised." The Orange Book further states "their effect is, by definition, 'after the event' so they are only appropriate when it is possible to accept the loss or damage incurred. Examples include [...] post implementation reviews."

  The Government of South Australia refers to an additional control type:
    - Motivational controls, such as supporting leadership, promote team spirit and offer training actions that "create the right environment for things to happen."
- Transfer, when the organisation outsources the risk to a third party – typically an insurance company. This by itself does not prevent an event from happening, nor does it reduce the consequences of the event. In such cases the insurance company pays a compensation to the insured company, enabling them to cope with costs incurred after the occurrence of the event. There are several books fully dedicated to the subject, such as the industry-neutral "Risk Management & Insurance", by Harrington and Niehaus (Harrington & Niehaus, 2003) or the aviation-specific

"Introduction to Aviation Insurance and Risk Management" by Wells and Chadbourne (Wells & Chadbourne, 2007). It is impossible to transfer all risks: either because the insurance company does not cover specific items, or to accept them it charges premiums that are too costly. Also, as the total mandatory and optional insurance costs represent a significant portion of any organisations' operating costs, the sensible management of the insurance portfolio requires dedication, knowledge and business sensibility.

- Terminate, when the organisation chooses to cancel a specific risk, thus it won't be further exposed to it. A good example is closing a business unit in a particular country, ahead of political, economic or social changes arising that might lead to turmoil, physical damage or nationalization. By withdrawing from that market the organisation will lose business, but will also not be exposed to any new risk there. This option is not always applicable, notably when established contracts regulate the continued operation regardless of surrounding conditions. Nevertheless, exit options should always be included and foreseen in commercial relationships.
- Take the opportunity, e.g. when other mitigation measures expose opportunities that could be harvested, enhancing market positioning and business performance.

In any case the organisation should have *reasonable assurance* that selected risk treatment and selected control measures are proportional to the risk itself (HM Treasury, 2004).

An example of risk controls in action can be found in the figure below, where for each given risk and inherent assessment several controls can be put in place to mitigate the consequences of each risk. While not covering 100% of the consequences, they may leave residual risks uncovered which the organisation (or individual) may decide to take or not.

Figure 31: Sample risk controls

OBJECTIVE – To travel from A to B in time for an important meeting								
	Inherent assessment		CONTROLS IN PLACE	Residual assessment		ACTION PLANNED	TARGET DATE	OWNER
RISK	Impact	Likelihood		Impact	Likelihood			
Missing a train makes me late for the important meeting	High	High	Catch train one earlier than I actually need	High	Low	No further action planned		M.Y. Self
Severe weather prevents the train from running	High	Low	Cannot control	High	Low	Telephone conferencing facility to be installed as a contingency	August	A.N. Other
Engineering works make the train late	High	Medium	Check for engineering works and arrange flexibility with people I am meeting	Medium	Low	No further action planned		M.Y. Self

Source: (HM Treasury, 2004, p. 41)

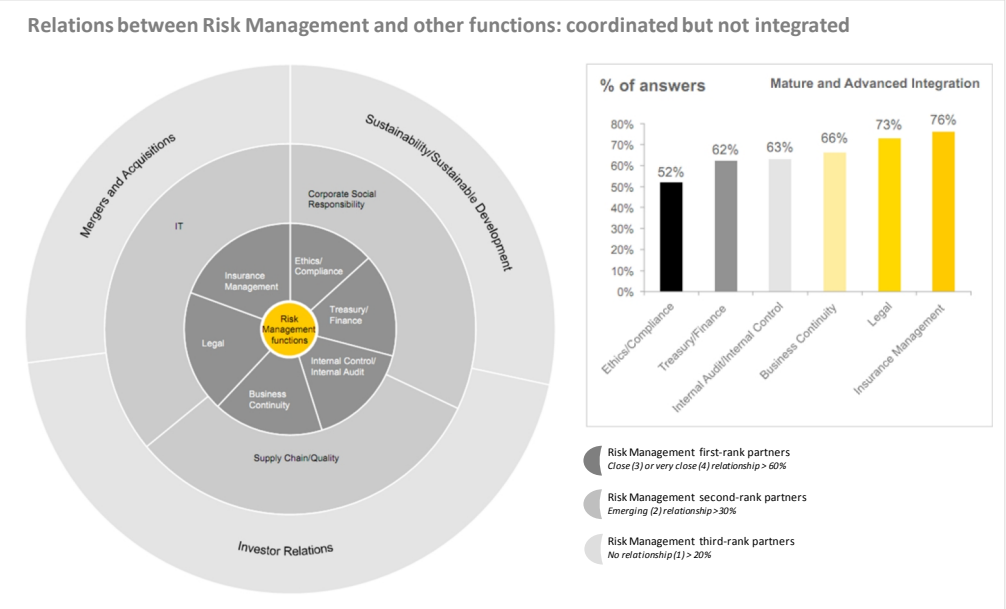
2.4.7. Organisational aspects on risk management

In a survey conducted by the Federation of European Risk Management Associations (FERMA), covering over 800 companies, risk management has been classified as one of the central functions of management, and should therefore be coordinated with other corporate functions. The most directly related functions include (multiple choice question):

- Insurance Management, selected by 76% of respondents (possibly indicating that risk management still goes through subscribing insurance packages),
- Legal, mentioned by 73% of respondents,
- Business Continuity, chosen by 66% of participants,
- Internal Audit / Internal Control, collected just 63% of answers (the use of 'just' will be justified later in this section),
- Treasury/Finance, 62% and
- Ethics/Compliance, 52% (which is surprising as compliance should be understood as one of the elements of risk management itself).

In a second level, Corporate Social Responsibility, IT and Supply Chain/Quality are mentioned.

Figure 32: Risk Management vs other management functions

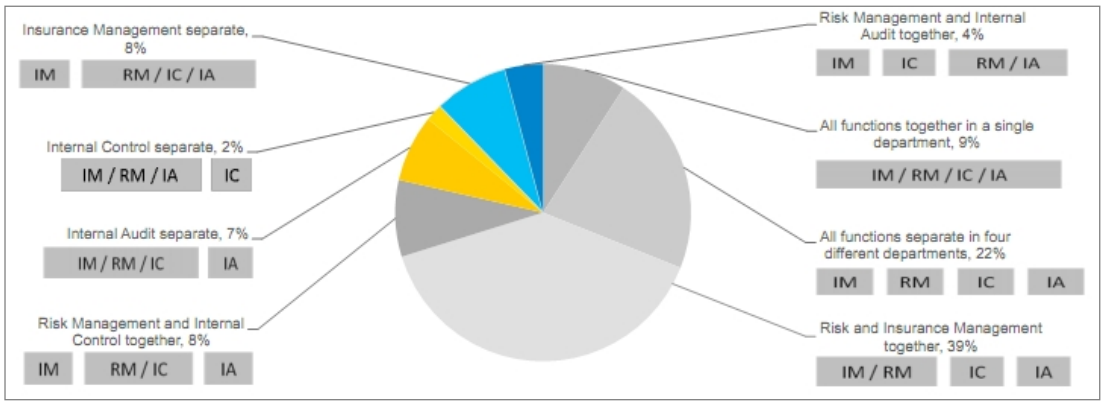


Source: (FERMA, 2012, p. 43)

When asked about how these functions are organised within their own companies 39% say their Risk and Insurance Management functions are integrated in one unit, while Internal Control and Internal Audit are kept separate. 22% say the four functions are separate within their organisation.

The full integration of all four functions into a single department is mentioned by 9% of respondents. Other organisational models, with a variety of other combinations are chosen by the remaining participants.

Figure 33: Risk Management organisation

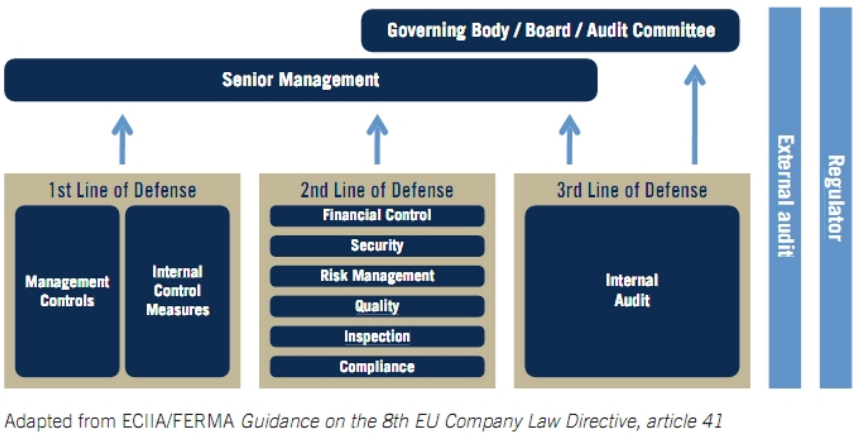


Source: (FERMA, 2012, p. 22)

Earlier on a statement of surprise was made on the limited number of respondents choosing Internal Control / Internal Audit as a function related to Risk Management. Adding up all companies that have Risk Management integrated with either Internal Audit or Internal Control, or both together, in one single department, 38% have these functions merged into one unit.

Moreover, FERMA and the European Confederation of Institutes of Internal Auditing (ECIIA) produced a common guidance on the 8th EU Company Law Directive – article 41, where Internal Audit and Internal Control seem to assume a rather important position in the so-called “three lines of defence model” for effective risk management and control.

Figure 34: The three lines of defence model



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

Source: (Institute of Internal Auditors, 2013, p. 2) and (FERMA, ECIIA, 2010, p. 7)

Recalling, the 8th EU Directive in its article 41 states: “each public-interest entity shall have an audit committee. [...] The audit committee shall, inter alia: (a) monitor the financial reporting process; (b) monitor the effectiveness of the company's internal control, internal audit where applicable, and risk management systems; (c) monitor the statutory audit of the annual and consolidated accounts; (d) review and monitor the independence of the statutory auditor or audit firm, and in particular the provision of additional services to the audited entity” (European Parliament and European Council, 2006).

It is therefore clear that Internal Audit and Audit Committee are supposed to be separate entities within a company, the latter assuming the monitoring of the companies risk management effectiveness. Ultimately the Audit Committee reports to the Board of Directors, hence their involvement in the third line of defence.

Figure 35: Roles and responsibilities in risk management

FIRST LINE OF DEFENSE	SECOND LINE OF DEFENSE	THIRD LINE OF DEFENSE
Risk Owners/Managers	Risk Control and Compliance	Risk Assurance
• operating management	• limited independence • reports primarily to management	• internal audit • greater independence • reports to governing body

Source: (Institute of Internal Auditors, 2013, p. 6)

This is in line with the Turnbull Report published in the UK in 1999 and updated in 2005. It is stated: “The board of directors is responsible for the company's system of internal control. [...] The board must further ensure that the system of internal control is effective in managing those risks in the manner which it has approved” (FRC, 2005, p. 6).

Also “the board's deliberations should include consideration of the following factors:

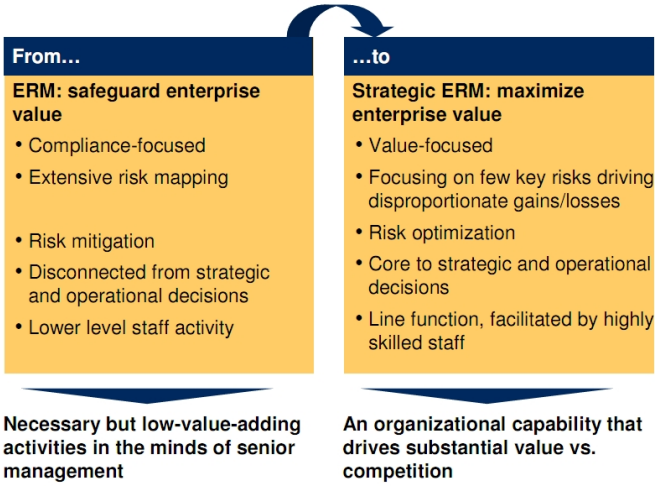
- the nature and extent of the risks facing the company;
- the extent and categories of risk which it regards as acceptable for the company to bear;
- the likelihood of the risks concerned materialising;
- the company's ability to reduce the incidence and impact on the business of risks that do materialise; and
- the costs of operating particular controls relative to the benefit thereby obtained in managing the related risks” (FRC, 2005, p. 6).

In the paper produced by McKinsey's Brodeur and Pritsch, which is also based on a survey conducted to US-based companies in the context of a conference on "The Role of the US Board of Directors in Entreprise Risk Management" held in New York in 2006, key conclusions are: "risks should be overseen by the full board, managed by line management, and discussed freely in multiple forums" (Brodeur & Pritsch, 2008, p. 6).

Despite being placed at the top of the organisation, the actual execution of risk management activities should be done by line management. This is also coherent with the three lines of defence model presented earlier.

Brodeur and Pritsch also suggest that the typical Enterprise Risk Management should evolve from safeguarding a companies' value to maximising its value, focussing the exercise more on value creation rather that compliance fulfilment. The first is understood to add low value to the company, while the second optimise risk and risk management to create measurable value for the operation and business performance.

Figure 36: Strategic shift in Enterprise Risk Management



Source: (Brodeur & Pritsch, 2008, p. 5)

Both Sadgrove and Coleman concur.

Sadgrove states: "the board should discuss the big risk management issues, since that is where the strategic decisions are made. Board members should: know the organisations' attitude to risk, [...] be aware of major risk issues in the business, receive regular reports on risk, including internal audits and challenge management's preconceptions, cultural norms or received wisdom on issues relating to risk" (Sadgrove, 2005, p. 44).

Coleman takes this one step further and proposes the Chief Risk Officer (CRO) position to manage the whole risk management process within the organisation. In his words, the CRO objectives are to "provide leadership for ERM, [...] coordinate internal and external risk reporting, [...] establish baseline measures of firm performance, such as milestones and indicators of best-in-class outcomes, [...] ensure compliance with stock exchange and regulatory requirements for risk management, [...] to better incorporate risk into the firm's strategy and programmes" (Coleman, 2009, p. 131).

Finally Pritsch, Stegemann and Freeman summarise risk management in the following terms: "Good risk management is based on getting four basic disciplines right:

- Ensuring full transparency across all risks and across the organisation.
- Putting in place vigorous risk governance structures.
- Clearly defining (and ensuring compliance with) the firm's risk appetite,
- Instilling a consistent, strong risk culture focused on optimizing well-understood risk return trade-offs within the defined risk strategy."
  (Pritsch, et al., 2008)

2.5. Why traditional risk management fails

There may be many models, tools and instruments to manage risks (some of which will be presented and discussed in next chapters), but it is essential to be aware of what can fail in such processes, especially what can fail in the understanding of the generic definition of risk itself. Entire books have been written on the failure of risk management (such as Douglas Hubbard's *The Failure of Risk Management - Why It's Broken and How to Fix It* and Nassim Taleb's *The Black Swan – The Impact of the Highly Improbable*) and many papers discuss elements of what went wrong. This section will outline what literature presents as key reasons for failure.

From a general perspective, Taleb's argument is around the so called *black swan* or the *unknown unknown*, the highly unlikely event. He says that one cannot manage what is not known. So 'knowing' as much as possible is the best way to hedge any risk. Yet full knowledge, information, certainty, correctness and completeness are virtually impossible. The world is dynamic, things change beyond an individuals' will. Therefore, the unexpected can and will happen. "The rarer the event, the less we know about its odds. It means that we know less and less about the possibility of a crisis" (Taleb, 2007, p. 226).

Taleb's *black swan* is defined as an outlier that carries an extreme impact. As it is so rare, there is no history or record on its impact so that "human nature makes us concoct explanations for its occurrence after the fact, making it explainable and predictable" (Taleb, 2007, pp. xviii - prologue). What makes organisations fail to identify, understand and address this *black swan* is what Taleb calls blindness to the black swan. He summarises this blindness into points such as "we behave as if the black swan does not exist", "what we see is not necessarily all that is there" and "we focus on a few well-defined sources of uncertainty" (Taleb, 2007, p. 50).

So when quantitative approaches suggest probability analysis around averages and normal distributions is sufficient to analyse all possible risks, not focussing on the tails of that probability distribution can bring unpleasant surprises – and in this case the object has been quantitatively analysed. What is even more difficult to manage, is an event for which there is no history, hence no possibility to produce statistical analysis and thus forecasts based on the past. That is why Taleb suggests taking care with forecasts and forecasters, as most of their work is based on past events and probabilities that try to eliminate uncertainty.

Bernstein referred to this as the *mumbo jumbo* mentioned earlier. Yet, on another note, he suggests that "if everything is a matter of luck, risk management is a meaningless exercise. Invoking luck obscures truth, because it separates an event from its cause. [...] The essence of risk management lies in maximising the areas where we have some control over the outcome, while minimising the areas where we have absolutely no control over the outcome and the linkage between effect and cause is hidden from us" (Bernstein, 1996, p. 197). So, visibility over events and its causes is a key element for managing risk.

Unsurprisingly, René Stulz lists six ways companies mismanage risk, starting with the reliance on historical data (Stulz, 2009, p. 4). In detail:

- "Relying on historical data;
- Focusing on narrow measures;
- Overlooking knowable risks;
- Overlooking concealed risks;
- Failing to communicate;
- Not managing in real time."

Having information, acting upon in a timely and complete manner, communicating properly what is at stake and what will be done are, according to this author, key elements to avoid

mismanaging risks. Certainly, finding the right model and manager to handle this complexity is of utmost importance for an organisation that wants to succeed.

Hubbard lists seven challenges for risk management (Hubbard, 2009, p. 76) that, when not tackled soon and properly, can naturally lead to the failure of this specific risk management approach. They are presented and debated below:

1. "Confusion regarding the concept of risk", stressing the importance for individuals within an organisation, therefore the entire organisation as a whole, to have and use a common language and definitions of elementary risk concepts. For example, ISO's Guide 73 is a good starting point and should be widely adopted.
2. "Completely avoidable human errors in subjective judgements of risk", leading to a potentially understatement of risk. While it is impossible to have fully quantitative analysis on any risk item, it is also not possible to only rely on qualitative analysis. This leads to subjectivity and therefore volatility of opinions, some based on simple errors originated in wrong judgements. [5]
3. "Entirely ineffectual but popular scoring methods." Hubbard is very outspoken against false quantifications of scoring risks in 1-5, or low to high categories, based on momentary interpretations of a person or panel of persons. Some of the analysis methods presented above rely on such scores, either because it is the most simple way to evaluate a risk or because the organisation lacks any efficient manner to quantify its probability. Important here is to stress that the organisation, when choosing such a method, is aware of its flaws and weaknesses.
4. "Misconceptions that block the use of better, existing methods." Although self explanatory, this can also be seen as a contradictory statement: if organisations confuse risk concepts and don't use a common language (challenge 1, above) how can they know all methods and choose the best to manage risk. Or, when knowing all those options, having the best might not be viable for one organisation, due to cost, resource availability or complexity reasons.
5. "Recurring errors in even most sophisticated models." Hubbard cites limited quality control and reality check efforts when implementing and using such methods, or even lack of training to fully exploit the full capabilities of the chosen model. One might say what leads to these errors is the over reliance on the model and its supplier, due to the inherent sophistication. The overreliance on statistics and tools is also quoted by Martin Pergler and Andrew Freeman at McKinsey leading to the 'garbage in, garbage out syndrome': "Those who place too much faith in sophisticated modelling get overambitious, and eventually get punished by fate", they say (Pergler & Freeman, September, 2008, p. 5).
6. "Institutional factors" such as "isolation of risk analysts from each other, within the same organisation or among organisations". This is the typical silo approach so

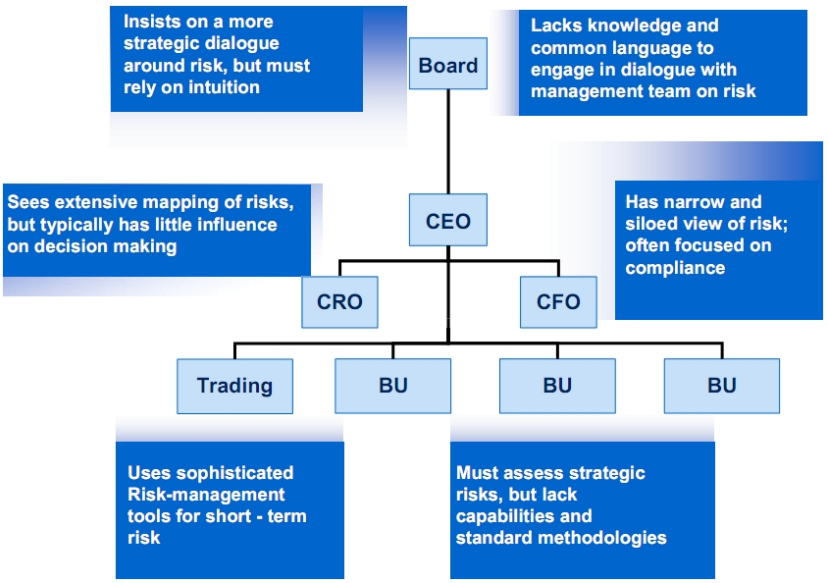
[5] Hubbard would certainly rebate statements of impossibility of measurement – he dedicates an entire book to that: *How to measure anything: Finding the Value of Intangibles in Business*, Wiley 2010.

common in many fields, not just risk management, leading to lack of communication and cooperation in managing key issues of the organisation.

7. "Unproductive incentive structures." Hubbard states "the methods will not matter much if the incentives to make better decisions and manage risks are not improved" linking better risk management (or any other new task) must be rewarded and compensated as way to stimulate motivation and engagement from the employee. This suggests that there is an inherent unwillingness to cooperate or that this cooperation and task performance can only be achieved if properly incentivised, which is highly debatable in the current social and economic climate.

On top, from an organisational perspective, there is always the possibility that risks and respective management actions are ignored, postponed or forgotten. Kevin Buehler, Andrew Freeman and Ron Hulme developed further reasons for failings in risk culture (Buehler, et al., 2008). These can be viewed in the figure below.

Figure 37: Common failings in risk culture



Source: (Buehler, et al., 2008, p. 34)

What can be seen from here is that the sources for mismanaging risk can be anywhere within the organisation:

- At board level, when knowledge and/or a common language is missing, or when elements of the board insist on a more strategic dialogue around risk relying mostly on intuition rather than facts and analysis supplied by management (it is possible to establish here the link to what Bernstein suggested as the *gut feeling* in addressing risks);
- At Chief Executive Officer and Chief Financial Officer level, when these have a narrow and silo view on risk, focusing on compliance issues only and missing the bigger picture of issues outside of their visibility radius;

- At Chief Risk Officer level, when there is too much focus on the detail as there is full visibility over the extensive mapping of risk but have little influence on decision making;
- At lower levels, when strategic risks must be assessed, but there is a lack of capabilities and standard methodologies, despite using sophisticated tools for short-term risk.

Hubbard's analysis and conclusions underline this. He even identifies a *risk paradox*: "The most sophisticated risk analysis methods used in an organisation are often applied to low-level operational risks, whereas the biggest risks use softer methods or none at all" (Hubbard, 2009, p. 175).

When talking about risk management models, Hubbard asks a very blunt but simple question: "how do you know it works?" whenever organisations suggest their risk management model is perfect (Hubbard, 2009, p. 13). One never truly knows if all risks have been identified, let alone treated, until the actual critical event has happened and put the model to a test. If at that point the organisation folds, one immediately knows the model did not work properly. On the other hand, if an event has been properly identified and treated that does not mean that all others have or will be handled similarly well.

Some interviewees (see later chapters) come to the conclusion that if an organisation has survived for decades or even centuries, then one can surely say that - over the past - they have managed their business and all associated risks properly. In any case, that alone is no guarantee that it will continue doing well over the near or distant future. This underscores the need for a constant effort to identify and manage risks the organisation might face.

Therefore, as can be seen in the comments made by Stulz, any risk management effort must be *complete* (Stulz, 2009, p. 4). Hubbard proposes four completeness checks to test the risk identification method chosen by an organisation, justifying it: "A risk manager should always assume the list of considered risks, no matter how extensive, is incomplete. All we can do is increase completeness by continual assessment of risks from several angles" (Hubbard, 2009, p. 47). The four checks are:

- Internal (functional) completeness, making sure that the entire organisation is involved and included in the risk management effort, not excluding any area from the assessment.
- External completeness, looking at direct and indirect stakeholders involved, related or just interested in the organisation, how they are affected by or can affect the organisation.

- Historical completeness, looking into how past events affected similar organisations in the same region or industry. “There is no reason to believe they can’t happen again” (Hubbard, 2009, p. 48)
- Combinatorial completeness, analysing how events from different natures and origins can produce heightened effects when happening consequently caused by each other or randomly together. This is probably the most exhaustive and complex check, but it allows organisations to have various perspectives on its operations and identify what can affect its performance.

Of course, if organisations adopt off-the-shelf risk management solutions, without adapting it to their own needs and requirements – of organisational, geographical or industry-specific nature – than sooner or later this model will prove to be inadequate and lead to the failure of the risk management effort.

2.6. Aviation-specific risk management literature

Very few authors have consistently dedicated their research to the management of risk in the aviation industry, therefore the number and quality of industry-specific risk management literature is limited. Without aiming at being exhaustive, this section explores contributions some authors made to studying how risk management is being performed at airlines or how an industry-specific risk model should be tailored.

The most productive author is Ayse Kucuk Yilmaz, at Anadolu University in Turkey having produced, alone or in cooperation with Triant Flouris (Dean School of Aviation Sciences, Daniel Webster College, Nashua, USA), a total of four books and a number of papers in academic journals and conferences, beyond documents for other industries or industry-neutral literature.

In “The Best Entreprise Risk Management Practice for Airline and Airport Business” (Yilmaz, 2008), the author replicates available risk management standards and their descriptions, as well as case-by-case risk management practices at seven international airlines (Lufthansa, Continental Airlines, Delta Airlines, Finnair, Austrian Airlines, Silverjet and Jetblue) and two airport companies (FRAPORT AG, TAV Airport Holding Co). Information presented is mostly sourced from airlines’ and airports’ websites and reports, with no critical assessment or judgement thereof. No conclusion is drawn on “the best” Entreprise Risk Management (ERM) model used at airlines as the title suggests. As for airports, the author describes the existing practice at the two sample airports and tests an Analytical Network Process model (ANP) to quantitatively evaluate which of the two airport operators uses the best ERM-

process. This ANP methodology is described in one sentence: “ANP provides a more generalized model in decision-making without making assumptions about the independency of the higher-level elements from lower-level elements and also of the elements within a level” (Yilmaz, 2008, p. 181). Objective and subjective criteria enter this evaluation, leading to the conclusion that FRAPORT’s ERM model is “the best”.

Other publications by this author explore sustainability issues in aviation risk management, suggesting an Entreprise Sustainability Risk Management concept as a “framework for optimum risk management” (Yilmaz & Flouris, 2010a), without describing what *optimum* means in this context. This concept enlarges existing ERM models by adding the “triple bottom line” aspects such as financial, social and environmental. The figure below presents this ESRM model that the authors describe as “guidance to managers on how to establish a holistic and systematic sustainability risk management process that generates the risk indicators, risk sources, objectives, and reporting systems needed to ensure effective handling of sustainability risks and improved overall organisational performance and value” (Yilmaz & Flouris, 2010a, p. 5).

Figure 38: The Entreprise Sustainability Risk Management conceptual model

Source: (Yilmaz & Flouris, 2010b, p. 6)

This model is industry-neutral therefore the authors try to adapt it to the airline environment, describing for each of the mentioned steps what elements are required to fulfil the task in this industry. What was “define strategy, targets and plans” becomes “define airline strategy, targets and plans”; or what was “assign risk management committee” becomes “assign airline’s risk management committee” (Yilmaz & Flouris, 2010a, pp. 7-8), without ever detailing exact aviation-specific elements, making the link between the proposed ESRM model and its adaptation to aviation very weak.

If on one hand this model seems simple (if not simplistic), it is also redundant with other risk management standards already available in the market. As will be discussed later, COSO's and ISO's models are comprehensive, covering not only all productive, administrative or managerial areas of a company, regardless of their industry, but also their interfaces and dependencies to internal and external stakeholders. As is rightly said by Yilmaz and Flouris, sustainability is a key element in current management practices, and therefore it is already included in a wide-ranging and holistic risk management exercise. Pointing it out in a specific model is unnecessary and ineffective. What is probably needed is to explain how such a model can work within the airline environment, therefore in what industry-specific framework such an industry-neutral model can work.

Ünal Battal, also from Anadolu University, published a paper on Financial Risks at Turkish Airlines (Battal, 2008). Therein the author describes the status quo of Turkish Airlines, some financial and non-financial elements within the company (such as fleet structure and development plans, foreign currency positions, credit levels, liquidity and capital positions), without ever applying any of the known risk management models or any qualitative or quantitative evaluation techniques to judge the decisions made by Turkish Airlines. It is an interesting paper, but adds little or no substance to the risk management subject itself.

Another document looking into financial risks in the airline industry has been produced by Geoffrey Loudon, citing evidence from Australia and New Zealand. This, on the other hand, makes a true quantitative analysis of several variables and risk mitigation strategies – such as currency or fuel hedging – of the airlines analysed. He comes to the conclusion that "Airline management policy usually states that derivatives are not used for speculative trading purposes. However, whenever hedging is not complete but contains discretionary elements, the distinction between hedging and speculating becomes blurred." Therefore: "airlines examined in this paper more effectively manage their exposure to financial risks in the short term than in the long term. This is consistent with the usual notion that readily available hedging instruments are of limited help in managing long-run risks. However, we qualify this conclusion by noting that short-horizon returns may contain too much noise to detect true exposure levels" (Loudon, 2004, pp. 306-314).

So what Loudon suggests is that no financial hedging can truly cover and mitigate long-term risks, and even in the short-term results of mitigation strategies might be influenced by other elements beyond the management's control. This is an interesting conclusion that

underlines the example of Singapore Airlines presented earlier where, due to their fuel hedging strategy, heavy losses had been incurred during periods of economic distress not only in the country but especially at a global level.

Other academic reports on the subject include Sharon Fernando's *Risk Management Practices in the Airline Industry* (an MA Thesis at Simon Fraser University, Canada, produced in 2006) and Ng Ying Chow's Developing a Methodology in *Aviation Risk Management based on Susceptibility* (an MSc Thesis at the University of Science Malaysia, produced in 2007). Fernando's report lists and discusses risk management practices on 15 airlines from various regions, but does not go into further risk management modelling (Fernando, 2006). Chow's report launches the concept of susceptibility and applies this in the context of risk management, then applying it to Malaysian Airlines as a case study (Chow, 2007).

A doctoral thesis produced by A. El-Ashry at City University London in 1986 entitled *Aviation Risk Management*, addresses mostly flight operations and airworthiness issues linking these to risk identification and mitigation. At the time, holistic risk management models did not exist, nor does the author produce any suggestion on how such a model could be designed and implemented. Regardless of the contents and quality of the document, it is one of the precursors of all academic documents found on the subject.

Wells and Chadbourne produced "Introduction to Aviation Insurance and Risk Management", presenting the object of risk in the context of insurance. This 500-page book summarises the risk management chapter in less than 20 pages, half of which containing tables and definitions for insurance coverage purposes. How insurance and risk management are interrelated, what role insurance assumes in a risk management process or what positive or negative influence one has on the other is not addressed. While being a good reference guide for aviation insurance topics, the relevance for risk management is minimal. Yet, as seen above, many companies still approach risk management as a function of insurance and integrate this function into one unit within the companies' organisation.

Mark Salter linked the subjects of risk and aviation security, suggesting "aviation security is an accidental by-product of national security" (Salter, 2008, p. 246), as one results from increased actions against terrorism acts using aircraft and other civil aviation objects as targets. The paper is an analysis of the 9/11 Commission reports and their conclusions, therefore focussing only on aviation security issues as one single risk factor and how the increased attempts to control passengers and cargo can impact international trade and

mobility. The author manages to debate several issues related to risk management and aviation security coming to interesting conclusions: “International mobility is not something to be eliminated within this system, but rather the risk is managed to allow for the disposition of certain enterprises, forces, and knowledge. [...] The justifications of risk factors and security threats are different and produce different effects in terms of what can be governed in their name. Campbell makes this point: ‘not all risks are equal, and not all risks are interpreted as dangers. Those events or factors that we identify as dangerous come to be ascribed as such only through an interpretation of their various dimensions of dangerousness’” (Salter, 2008, pp. 247-253).

Salter makes a very critical analysis of current risk management practices in the specific fields of aviation security. Further on he suggests that “risk is used by airport and air carriers to pressure governments to spend more on aviation security [...]Risk is also used to manage passenger and stakeholder expectations. Several air carriers now announce that it is their policy that passengers remain seated, that the washrooms in the first-class cabin are reserved for first-class passengers for security reasons, and that crowding near the cockpit is prohibited. [...]While these controls are framed in the language of risk, they are justified through the appeal to the maintenance of security (not the reduction of risk)” (Salter, 2008, pp. 247-253).

In a further statement, Salter says: “Within the aviation security field, several competing consultancies have established models of risk analysis for terror attacks, which are promoted at regional and international industry conferences. Both the International Civil Aviation Organisation (ICAO) and the International Air Transport Association (IATA) are moving towards ‘enterprise risk management’ and ‘security management systems’ that are based on quantifiable security and ROI (return on investment) results.” Therefore “Risk management is an absolute empirical failure in providing real knowledge or increasing aviation security. But, it is a success for the *dispositif* of security: it continually generates new areas to which security might be applied” (Salter, 2008, p. 257).

Other books address the subject of risk management in the sidelines of their main themes. *Beyond Airline Disruptions*, by Jasenka Rapajic, discusses airline scheduling disruptions and their impact on the operation. This is just one possible risk factor and several causes can contribute to its occurrence. The author states that “the process of disruption risk management is frequently too narrow and reactive. In too many instances, management

emphasis is traditionally focused on contingency planning for recovery from massive disruptions, rather than avoidance of costly business mistakes. Management systems and processes aimed at minimising disruption risks are designed mainly around the operational rather than the corporate level." (Rapajic, 2009, p. 129) Further on the author suggests the airline should have enough understanding of the business, the risks faced, it should communicate how much risk it is willing to take and address the operation accordingly.

While not being on risk management or even risk identification, *Stormy Skies* by Paul Clark, is all about issues that affect airlines on a broad and strategic level. The author addresses issues such as past events critical to the airlines' historic performance (like economic crisis, diseases, explosive regional growth, etc.), forecasting issues, changing customer requirements, growing environmental issues, consolidation trends, and many others. All this is a valuable contribution to locating an airlines' position among the variety of issues that affect the industry and its own existence. No risk management models are discussed, nor mitigation strategies for each of those – that is not the purpose of the book.

2.7. Chapter Summary: inputs for the research process

The above sections summarised relevant literature on risk, its definition and concept, cultural aspects and related risk management theory. It has been seen that plenty industry-neutral material is available, but little aviation-specific documentation with sufficient quality and depth in covering holistic risk management topics has been published. This gap is one of the drivers to pursue the present research in the airline industry.

Controversy arises when looking at the statements made separately by Beck, Bernstein, Taleb and Hubbard. While some refer to the impossibility of having solid historic data covering all sorts of risks, thus "the impossibility to capture objective risk" as mentioned by Beck, others go the extreme of saying that everything is measurable, suggesting quantitative methods to evaluate every individual risk event.

It is relevant to stress that, as per the authors quoted in this chapter that it is impossible to reduce risk to zero, thus some sort of risk will always remain. Moreover, in some cases, the risk event itself is not manageable therefore the focus should be set on mitigating and managing the consequences of that particular risk event. This also leads to the conclusion that the organisation should perform a prioritization exercise to focus on key risks, rather than trying to tackle all risks it has identified. Since resources are limited and time is scarce,

focussing on what matters most is essential. Accepting that in this prioritisation process, some events that may occur can go unmanaged is a fact that the organisation needs to understand and accept as part of the risk management process.

Hubbard has identified several reasons contributing to the failure of risk management. The ineffectual scoring methods is one, but nevertheless, as will be seen later, some airlines keep using these methods – mostly for simplicity reasons, as they are easier to understand and implement. Other reasons listed include the lack of support and understanding by upper management. It may be a cultural issue: from the individual, the corporation or the society in which it is embedded where individual risk events may or may not be perceived as critical. At the end, quoting Beck, “risk depends on decisions” and this makes it an organisation problem, more than an individualistic one. Decisions taken by a group of people (say at executive management level) can contribute to the dilution of responsibility when it comes to taking (or not) specific risk related decisions.

Further concepts such as risk appetite, cascading risks, escalation and delegation of risk management responsibilities, risk maturity and the generic risk identification and mitigation techniques addressed above have also been taken into consideration for the design of an airline-specific risk management model. This model shall act as flexible guideline from which airlines can adopt the elements that are applicable to its own operation and with which they feel most comfortable with.

In terms of organisation, any risk management unit should be separate from internal audit functions. One of the later chapters shows how airlines have organised themselves, sometimes contradicting the separation principle mentioned above.

The following chapter will proceed with the description of the methodological approach used in this project.

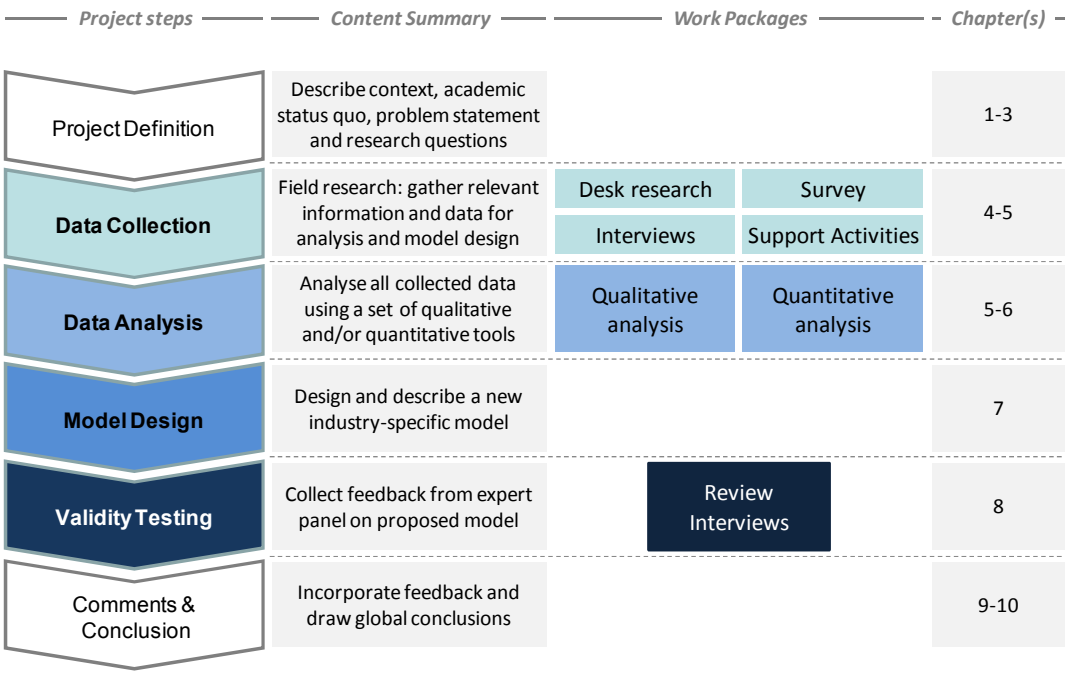
3. Methodology & approach

To achieve the outlined project objectives and answer research questions listed earlier, the designed methodology includes a number of sequential project steps and work packages. All combined they have allowed analysing the topic from various perspectives, also collecting quantitative data and qualitative information. These project steps and work packages are described in this section of the thesis. Given the professional motivation underneath this research, the chosen approach aimed at being as close to the air transport industry as possible, involving airlines, industry experts and related entities from the air transport value chain. Some of the initially foreseen initiatives had to be adjusted due to lack of feedback, cooperation or interest from contacted counterparts.

3.1. Global project approach

The overall approach followed a bottom-up sequence, gathering all possible information to understand existing shortcomings, identify possible improvement potentials and suggest ways to change status quo. Defining this approach, respective goals and objectives is part of the 'project definition' step, the first in the sequence depicted below (and already covered by Chapters 1 and 2 of this thesis). This included a review of existing literature, comprising industry-neutral and industry-specific documentation produced by academics and professional organisations.

Figure 39: Global project approach



The 'data collection' step comprises the core field work performed, via desk research, interviews, surveys and support activities. The content of each of these work packages is described in the next section. Goal was to collect as much empirical information from airlines and other aviation related entities, as well as some best practice examples from other industries. This data collection was made using primary sources (such as risk experts and key managers in the respective organisations) and secondary sources using relevant third-party publications, collected during the desk-research process or during the support activities performed (such as attending specialised courses and conferences – see next section). In the present document, the results of this step are compiled in Chapters 4 and 5.

After the collection of all available information, including the results of the planned field research activities, the 'data analysis' step aims at digesting, comparing and discussing information using a set of quantitative and qualitative tools. Goal was to identify where the improvement potentials are, understand how other industries are dealing with the same problems and discuss the viability of a tailor-made risk management model to the air transport industry. The results of this step can be found in Chapter 6 of the thesis.

Compiling all this fresh knowledge into an airline-specific risk management model was the task of the 'model design' step, covered by Chapter 7 of this document. This Chapter also lists the characteristics of such a new model, explaining its industry-specific features, suggest inherent work-steps and describe possible guidelines for implementation.

The model was subject to testing, by submitting it to industry experts for criticism and review[6]. Their renewed input and suggestions for correction are compiled in Chapter 8.

The last project step, 'comments & conclusion', aims at summarizing key findings of the entire research process by answering the listed research questions. Project contributions and limitations as well as suggestions for further research shall also be explored in the last chapters of this thesis.

[6] Ideally the model should be directly tested by implementation at one or more airlines willing to become case studies of the project, yet – and despite all efforts made – none of the contacted companies revealed themselves willing to cooperate in such a deeper level.

3.2. Work package description

As explained above, the various project phases foresaw work packages of different content and nature. The desk research process has set the tone for the remaining steps.

Figure 40: Desk research description

Desk Research	
Desired information	▪ What public information is available on current standards, methodologies and practices of risk management? ▪ Is there any publicly available information on how airlines are doing risk management?
Sources	▪ Books, papers, studies, websites on risk management ▪ Academic journals and newspapers with dedicated sections and articles on the subject
Work steps	▪ Collect, read, cross-check with other sources, contact authors, summarise information and produce own report

The desk research package aimed at gathering all publicly available information on the subject of risk, risk management, airline risk management practices, industry best practice, reports from other industries, etc. Sources were all possible documents, including books, papers, academic or industry journals, management reports and corporate studies, websites and newspaper articles. The most relevant documents were quoted throughout this thesis, and whenever possible, the respective authors were contacted to provide further details.

To complement the desk research information, key experts on generic and aviation specific risk management subjects were interviewed. There were three types of interview targets:

- Type A – Risk Professionals, targeting independent consultants, insurance companies, analysts and academic researchers with relevant work in the field of risk management. Goal was to complement the material gathered during the desk research process, cross checking information collected.
- Type B – Airline Representatives, targeting top responsible for risk management at airlines and other executives either in the fields of hedging, legal, insurance, etc.
- Type C – Other industries, targeting executives from other adjacent (e.g. Ground Handling, Airports) and unrelated industries with relevant experience in risk management. Goal was to gather lessons learned in these industries with the respective risk management models, to see how an airline specific model can be adjusted and optimised.

Figure 41: Interview target description

Interviews		
Type A Risk Professionals	**Type B** Airline Representatives	**Type C** Other industries
Who: ▪ Selected experts working in Risk Management, including consultants, insurance companies, academic researchers and others What: ▪ Current ERM practices Why: ▪ Complement material from literature review / desk research ▪ Get real life feedback on different models, implementation problems ▪ Hear the 'other side' external to the individual company	Who: ▪ Risk Managers and related airline executives with responsibilities in risk management (incl. if available CFOs, CEOs, CROs, others) What: ▪ Implemented risk management model within their airline Why: ▪ Learn if available models were replicable to the specific airline ▪ Understand what resources (human, technical, financial, time) are required	Who: ▪ Representatives and risk officers from other industries, adjacent or unrelated to air transport What: ▪ Specific risk management solutions Why: ▪ How are they doing it? ▪ What can be learned and transposed to airlines?

The review interviews considered in project step 'validity testing' took advantage of the contacts established during the regular interview process. Goal of this step was to validate the proposed new model with these experts.

The survey work package included a quantitative overview over current airlines' practices, using information collected from the Top 100 airline groups (based on revenue), as well as a review of other surveys on the subject of risk management at airlines performed by management consulting firms, independent researchers, etc.[7]

Finally, the supporting activities performed during the research process phase (and even before) aimed at complementing all above by attending conferences and training courses relevant for the subject. The training courses provided functional knowledge on risk management models, trends and implementation techniques both in industry-neutral and industry-specific environments. The conferences attended included academic events, where papers on aviation risk management-related subjects were presented (notably by Ayse Kucuk Yilmaz, one of the few airline risk researchers mentioned earlier) and industry-neutral events, such as a seminar by the Federation of European of Risk Management Associations (FERMA). A complete list of these supporting activities can be found in the figure below.

[7] The initial plan to run an online questionnaire to relevant managers at airlines around the globe, gathering quantitative and qualitative information from large, medium and small-sized airlines in all possible geographical locations, suffered from the lack of a consistent contact database and the lack of cooperation from contacted entities owning such databases.

Figure 42: Supporting activities attended

Support Activities	
Courses	**Conferences & Events**
Attend training courses dedicated to risk management, implementation techniques and practical aspects in industry-specific and industry-neutral environments	Attend academic and industry meetings where current status quo and/or new approaches to the subject are debated
▪ **Aviation Risk Management** Air Business Academy Toulouse, France – October 2007 ▪ **Managing Project Risk and Uncertainty** (module of MSc Project Management, Finance and Risk) City University London London, UK – 2010 ▪ **Practical Implementation of an Entreprise Risk Management Model** Portuguese Association for Quality Lisbon, Portugal – April 2011 ▪ **Risk Management according to ISO31000** Portuguese Association for Quality Lisbon, Portugal – June 2011 ▪ **Aviation Risk Management using ISO31000** Aerosafe Risk Management, via Airline Industry Association of New Zealand Wellington, New Zealand – November 2012 ▪ **Risk Management Foundations** (part of IATA Diploma in Integrated Risk Management) International Air Transport Association Singapore – May 2013	▪ **Air Transport Research Society world conference** 14th Edition ATRS Air Transport Research Society Porto, Portugal – July 2010 ▪ **World Conference on Transportation Research** WCTR Lisbon, Portugal – July 2010 ▪ **FERMA Risk Management Seminar 2012** *Living and Working in a riskier world* European Federation of Risk Management Associations Versailles, France – October 2012

Attending these helped not only in apprehending the most recent risk management practices in the industry, gaining more and updated knowledge for this project, but also in testing and cross-checking with lecturers and attendees preliminary ideas on model content and design. These events also provided an interesting network of risk management experts that can be used in various occasions during or after the conclusion of this project.

The following chapter proceeds with exploring the various risk management standards available, both in their industry-neutral and industry-specific versions.

– Intentionally left blank –

4. Available Risk Management Standards

Now that the basic concepts on risk have been laid out (see Chapter 2), it is relevant to briefly review the standards that have been developed at a national or international level to address and implement risk management practices in organisations. Several comparative studies[8] have been made before, so that more than producing another comparison of those, this chapter will look at the available standards, their interrelation with corporate governance and internal control approaches, highlighting their different definitions of risk. A special focus was placed on ISO 31000 – the latest and most internationally accepted standard – due to reasons outlined in section 4.2 below. Some aviation specific standards will also be analysed. The next chapter will then review the research results on current airline practices.

4.1. Corporate Governance codes and risk management standards

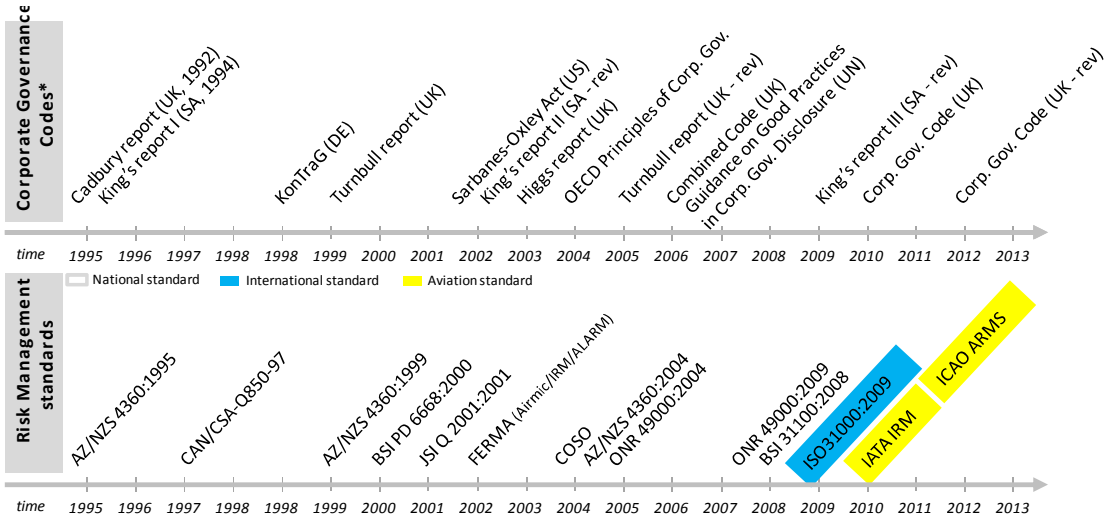
According to Sadgrove there are three ages of risk management (Sadgrove, 2005, p. 1) that, despite building on each other, have distinctive characteristics that show the development of management attitude towards risk. They are:

- The first age, is where companies managed risks mainly by subscribing to insurance policies. This was thus an incomplete way to manage risks, as not all risks were (and still are not) insurable and even when so, the respective insurance policy may not have covered 100% of the capital insured or have covered all consequences of the event if and when it happened. Risks never originated from managerial misconduct, rather from production incidents or security issues. Sadgrove places this age in the 1960's and 1970's.
- The second age, covering the 1970's and 1980's, was marked by the introduction of quality standards, leading to more consistent ways of production and management. Prevention was therefore introduced as way to manage risks, while complementing previously available insurance solutions. The focus was still on internal issues only.
- The third age started in 1995 with the publication of the world's first Risk Management Standard by the Standards Australia and Standards New Zealand organisations, the AS/NZS 4360:1995. The more preventive approach was kept, while focus was set on internal and external issues, with the companies' strategy being considered as key element to the risk management policy.

[8] Section 4.1 will provide more details on these comparative studies, which include (AIRMIC, 2005), (European Interagency Security Forum, 2010), (RIMS, 2011), (The Institute of Internal Auditors, 2010) among others

Several other risk management standards have since been developed and introduced, given the stronger requirements emanating from corporate governance and internal control guidelines developed by national and international bodies in parallel. The European Corporate Governance Institute lists a total of 386 corporate governance codes and guidelines published by national and international bodies (European Corporate Governance Institute, 2013). The below picture highlights the most relevant ones, starting with the Cadbury Report in the UK in 1992 and South Africa's Kings Report in 1994 (later updated in 2002 and 2009), listing also the appearance of risk management standards.

Figure 43: Overview of Corporate Governance Codes and Risk Management Standards



* Selection of Codes from 386 global documents listed by the European Corporate Governance Institute, www.ecgi.org

Source: adapted from (European Corporate Governance Institute, 2013)

The herein mentioned list of risk management standards is not exhaustive, but refers to the most popular ones. On a national level it includes the various updates of the Australian and New Zealand AZ/NZS 4360, the Canadian (CAN/CSA-Q850-97), British (BSI PD 6668:2000 and BSI 31100:2008), Japanese (JSI Q 2001:2001) and Austrian (ONR 49000:2009) standards. It also includes international standards such as FERMA's (based on the AIRMIC/IRM/ALARM versions of their joint risk management approach) and ultimately the ISO 31000:2009 as the latest international and industry neutral risk management standard, published in 2009.

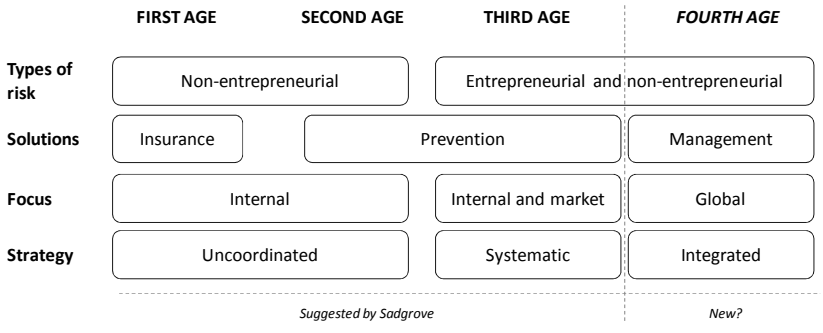
In 2010 IATA and ICAO, two international aviation bodies, released their own risk management guidelines, notably the Integrated Risk Management manual produced by the International Air Transport Association, (IATA, 2010)) and the Operational Risk Assessment approach by the Aviation Risk Management Solutions group of the International Civil

Aviation Organisation (ICAO, 2010). The aviation-specific standards will be addressed separately in one of the following sections of this chapter; as will the ISO 31000:2009 be further detailed, as the selected reference standard for this thesis.

The large volume of corporate governance codes is justified by the increasing events of organisational failures resulting from management misconduct, falsified reporting and misinterpretations of existing regulations all over the world. The Enron scandal, Worldcom or the several Ponzi schemes uncovered during the most recent financial crisis are just examples of that. As all these new codes require organisations to have improved reporting practices, more transparent governance models and visible risk management practices in place, it is no surprise that the number of risk management standards has increased over time, too. The depth and complexity of the various approaches has evolved, some being more integrated than others.

As possible extension to Sadgroves' three ages of risk management, the world is already in a fourth age of risk management, where the solutions are based on the complete management of risk, its sources and consequences, rather than "just" insurance and prevention. Furthermore, the focus is on the global risk landscape, regardless of the risk event being originated in the internal or external environment. Therefore corporate and risk management strategies must be integrated with each other in order to provide a truly enterprise-wide risk management approach, while being aligned with the corporate governance approach.

Figure 44: The revised ages of risk management



Source: adapted from (Sadgrove, 2005, p. 2)

The latest revision of South Africa's King Report dedicates an entire chapter to the governance of risk. The heavy reliance and responsibility of the organisations' board of directors is clearly visible, in order to ensure that there is a risk management model in

place, that it is consistently implemented throughout the organisation and that there is proper reporting of all activities. Ten principles are listed for good risk management:

- "Principle 4.1 – The board should be responsible for the governance of risk;
- Principle 4.2 – The board should determine the levels of risk tolerance;
- Principle 4.3 – The risk committee or audit committee should assist the board in carrying out its risk responsibilities;
- Principle 4.4 – The board should delegate to management the responsibility to design, implement and monitor the risk management plan;
- Principle 4.5 – The board should ensure that risk assessments are performed on a continual basis;
- Principle 4.6 – The board should ensure that frameworks and methodologies are implemented to increase the probability of anticipating unpredictable risks;
- Principle 4.7 – The board should ensure that management considers and implements appropriate risk responses;
- Principle 4.8 – The board should ensure continual risk monitoring by management;
- Principle 4.9 – The board should receive assurance regarding the effectiveness of the risk management process;
- Principle 4.10 – The board should ensure that there are processes in place enabling complete, timely, relevant, accurate and accessible risk disclosure to stakeholders." (Institute of Directors in Southern Africa, 2009)

Other – perhaps older – governance codes are less stringent when it comes to risk management practices. For example the Sarbanes Oxley Act, introduced in the United States as immediate consequence of the Enron scandal in 2002, has no explicit reference forcing companies to have a risk management system in place (Senate and House of Representatives of the United States of America, 2002). Instead, it focuses on internal control, requiring companies to state their internal control procedures in their annual reporting.[9] This is summarised in Section 404 of the Act, a few paragraphs that outline the responsibility of management in explaining the organisations' internal control efforts in their annual reporting documents.

To clarify this, the US-based Security and Exchange Commission issued in 2007 a 77-page interpretation and guidance document, clarifying the purpose and use of this section of the Sarbanes-Oxley Act, admitting that "it is possible to design into the process safeguards to

[9] It is relevant to distinguish internal control from risk management. The IRM, the Institute of Risk Management, together with AIRMIC, a UK-based organisation representing risk managers and buyers of commercial insurance, define risk management as "the forward looking executive role that anticipates and evaluates risks and ensures that efficient and effective controls are developed and implemented", while internal control "is primarily concerned with the monitoring of controls with oversight from the non-executive Audit Committee." (AIRMIC, IRM, 2009).

reduce, though not eliminate, this risk" therefore suggesting a top-down risk based approach to financial reporting (Securities and Exchange Commission, 2007, p. 3). In the meanwhile, the Committee of the Sponsoring Organisations of the Treadway Commission (COSO) finalised in 2004 their "Entreprise Risk Management – Integrated Framework" that quickly became the risk management standard used by US-based and stock listed companies, thus one of the most widely used and known standards for risk management (COSO, 2004).

Figure 45: Sarbanes-Oxley Act of 2002, Section 404

SEC. 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS.

(a) RULES REQUIRED.—The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall—

(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

(b) INTERNAL CONTROL EVALUATION AND REPORTING.—With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

Source: (Senate and House of Representatives of the United States of America, 2002, p. 789)

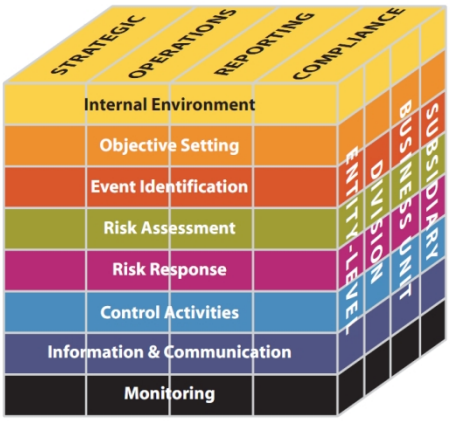
While apparently very simple, it is a broad approach that covers company-wide risk areas. The depiction of the process as a three-dimensional matrix is widely known as the COSO Cube (see Figure 46: The COSO Cube), showing that this approach is based on:

- Four objectives that the organisation tries to achieve – these being in the strategic, operations, reporting and compliance categories;
- Eight components as key elements for objective achievement – internal environment, objective setting, event identification, risk assessment, risk response, control activities, information & control and monitoring; and
- Four entity units (or more, or less, depending on the organisation) including the subsidiary, business unit, division and entity-levels.

The above-mentioned SEC guidance document does not specify COSO as being the only "suitable control framework", also suggesting the "Guidance on Assessing Control published by the Canadian Institute of Chartered Accountants ("CoCo") and the report published by the Institute of Chartered Accountants in England & Wales *Internal Control:*

Guidance for Directors on the Combined Code (known as the Turnbull Report) as examples of other suitable frameworks that issuers could choose in evaluating the effectiveness" of internal control and financial reporting (Securities and Exchange Commission, 2007, p. 11).

Figure 46: The COSO Cube



Source: (COSO, 2004, p. 23)

South Africa's King Report is not restricting the risk management approaches to the use of one specific standard, rather suggesting "for instance COSO, ISO, IRMSA ERM Code of Practice, IRM (UK), etc." as long as clearly stated in the companies' reporting as being used as guiding risk management framework (Institute of Directors in Southern Africa, 2009).

The IRM (UK) framework of the Institute of Risk Management is a joint development with AIRMIC, a UK-based organisation representing risk managers and buyers of commercial insurance. This has also been adopted in 2002 by the Federation of European of Risk Management Associations, FERMA, as their recommended approach.

As the most recent standard, and from beginning on adopted as guiding framework for this thesis, the ISO 31000:2009 (International Organisation for Standardisation, 2009a) will be further detailed in the next section. It is very much leaned to the Australian / New Zealand Standard, as the standardisation bodies of these two countries are clearly the precursors in drafting integrated risk management guidance material.

All these standards have their own risk management approach and definitions. As mentioned earlier, this thesis does not intend to produce a comparison of the various standards currently available, as many similar exercises have already been carried out by other authors.

A non-exhaustive list of such comparative reports includes:

- "An overview comparison of the AIRMIC/ALARM/IRM Risk Management Standard with the Australia/New Zealand Standard AS/NZS 4360:2004 and the COSO Enterprise Risk Management – Integrated Framework", by AIRMIC (AIRMIC, 2005);
- "A Comparative Review of Risk Management Standards" by Raz, Hillson (Raz & Hillson, 2005);
- The European Interagency Security Forum with an excel-spreadsheet comparing AIRMIC / ALARM / IRM 2002 against AS/NZS 4360:2004, COSO, ISO 31000 and BSI31100:2008 (European Interagency Security Forum, 2010);
- "The Executive Report on Widely Used Standards and Guidelines" by the Risk and Insurance Management Society, Inc. (RIMS, 2011);
- "The New International Standard on the Practice of Risk Management – A Comparison of ISO 31000:2009 and the COSO ERM Framework" by the IMA (The Institute of Internal Auditors, 2010).

The comparison produced by Raz and Hillson distinguishes negative, neutral and broad definitions of risk as presented by a number of project-based and organisation-wide risk management standards. According to these authors, a negative definition relates risk to negative events or even a threat in the foreseeable horizon; a neutral definition is the one that does not link risk to a positive or negative event; and a broad definition includes both positive and negative events into the risk definition (Raz & Hillson, 2005). Figure 47 summarises the various definitions in the three categories. As this paper was published in 2005 it does not contain the definitions used by COSO or ISO 31000:2009; therefore Figure 47 has been augmented to include these two additional definitions.

COSO's documentation is quite clear when it comes to defining risk and distinguishing this from events. "An event is an incident or occurrence from internal or external sources that affects achievement of objectives. Events can have negative impact, positive impact, or both. Events with negative impact represent risks" (COSO, 2004, p. 16). Therefore in the COSO environment risk has a negative weight.

On the other hand, ISO 31000:2009 clearly states that "this International Standard can be applied to any type of risk, whatever its nature, whether having positive or negative consequences" and that, when defining risk as "the effect of uncertainty on objectives", an "effect is a deviation from the expected — positive and/or negative" (International Organisation for Standardisation, 2009a, p. 1). It becomes clear that ISO 31000 has a more embracing attitude towards risk, therefore falling into the broad risk definition using Raz and Hillson's categorisation.

Figure 47: Definitions of risk

Original comparison by Raz and Hillson

Negative definitions	Neutral definitions	Broad definitions
CAN/CSA-Q850-97:1997: 'the chance of *injury or loss*'	AS/NZS 4360:2004: 'the chance of something happening that will have *an impact* upon objectives'	PMBoK® 2004: 'an uncertain event or condition that, if it occurs, has *a positive or negative effect* on a project objective … includes both *threats* to the project's objectives and *opportunities* to improve on those objectives'
IEEE 1540:2001: 'the likelihood of an event, *hazard*, *threat* or situation occurring and its *undesirable consequences; a potential problem*'	BS6079-3:2000: 'uncertainty … that *can affect* the prospects of achieving … goals'	IRM/ALARM/AIRMIC 2002: 'combination of the probability of an event and its consequence … consequences can range *from positive to negative*'
	IEC 62198:2001: 'combination of the probability of an event occurring and its *consequences* for project objectives'	PRAM Guide 2004: 'an uncertain event or set of circumstances which, should it occur, will have *an effect* on achievement of … objectives … *either positively or negatively*'
	JIS Q2001 (E): 'a combination of the probability of an event and its *consequence*'	

Additions to Raz and Hillson

COSO: 'Risk is the possibility that an event will occur and adversely affect the achievement of objectives.'	ISO31000:2009: 'effect of uncertainty on objectives'

Source: (Raz & Hillson, 2005, p. 64); added with respective risk definitions from (COSO, 2004, p. 16) and (International Organisation for Standardisation, 2009a, p. 1)

The comparative study produced by the US-based Risk and Insurance Management Society (RIMS) presents a summary of all standards, based on attributes relevant for their RIMS Risk Maturity Model. The compared standards include, beyond the aforementioned COSO, ISO 31000:2009, FERMA:2002 and BS 31100:2008, the OCEG "Red Book" 2.0:2009 (OCEG is a think tank founded to improve corporate compliance and ethics) and the SOLVENCY II:2012 document (a dedicated directive for the insurance industry published by the European Union). The seven attributes of the RIMS Risk Maturity Model are:

- Adoption of an ERM-based approach as element of the corporate culture;
- ERM Process Management, as indicator of the "incorporation of repeatable and scalable risk management process into all business and support units";
- Risk Appetite Management indicating the understanding of the concept and establishment of such a threshold within the organisation;
- Root Cause Discipline leading to the consistent analysis of sources of identified risks, their understanding and their impacts on other areas of the organisation;

- Uncovering Risks, looking into how risks are identified and reported;
- Performance Management, understood as the articulation between risk management and remaining management activities that contribute to the achievement of organisational goals and objectives; and
- Business Resilience and Sustainability, understanding how all activities contribute to the creation of long-term value for the organisation.
  (RIMS, 2011, p. 5)

Using this set of attributes the authors of the RIMS report come to the conclusion that the ISO 31000 standard is the most complete, together with SOLVENCY II, fulfilling all their requirements. The BS31100, a close relative of the ISO 31000 produced by the British Standards Institution, lacks fulfilment of the last attribute (Business Resiliency and Sustainability). COSO, FERMA and OCEG's models lack two attributes each, notably the Root Cause Discipline.

Figure 48: Overview of common elements of risk management standards

RIMS RMM ATTRIBUTE	ISO 31000	OCEG	BS 31100	COSO	FERMA	SOLVENCY II
ERM-Based Approach	X	X	X	X	X	X
Process Management	X	X	X	X	X	X
Risk Appetite Management	X	X	X	X	X	X
Root Cause Discipline	X		X			X
Uncovering Risks	X	X	X	X	X	X
Performance Management	X		X	X	X	X
Business Resiliency & Sustainability	X	X				X

Source: (RIMS, 2011, p. 23)

Given that SOLVENCY II is not industry neutral, but directed to the insurance business, the ISO 31000 is so far the only industry neutral standard that complies with all attributes of the RIMS Risk Maturity Model, underlining the relevance of this risk management standard.

The next section will therefore focus on ISO 31000, detailing its key elements and approach for risk management, as well as outlining the reasons why it has been chosen as the guiding risk management framework for this thesis.

4.2. Focus on ISO 31000:2009

From all available risk management standards, choosing ISO 31000:2009 as the reference for this thesis was the obvious and only possible choice. Reasons include:

1. Not only is it the most recent standard, but it is also – by definition and as standard of the International Organisation for Standardisation – internationally valid and recognized. The aforementioned paper by RIMS states "once ISO or a regional standards body adopts a standard, the individual national standards are dissolved. (...) The American National Standards Institute (ANSI), the Canadian Standards Association (CSA) and the Australian Standards (AS) and New Zealand Standards (NZS) organisations have all recently adopted ISO 31000:2009 as their respective national risk management standard" (RIMS, 2011, p. 24).
2. Moreover, unlike the SOLVENCY II example, ISO 31000 is industry neutral and flexible, having been implemented in many industries, geographies and company sizes. It should therefore be easily adaptable to the aviation environment, too.
3. As also seen before, it enables a holistic view of risks affecting the organisation, from internal or external sources, while considering risk an event with negative or positive effects (unlike COSO that only considers the negative aspect of the event).

This section will thus outline further details of ISO 31000:2009, such as its origin and purpose, core elements and understand how it is integrated with other ISO standards.

4.2.1. Origin and purpose

ISO's risk management standard started as an update to AS/NZS 4360:2004 by the Australian and New Zealand Standards organisations, but ended up being the first version of an international standard on risk management. Mr. Kevin Knight was nominated to chair the working group in charge of drafting the standard and then also to chair the Technical Committee 262 in charge of leading all discussions on standardisation in the field of risk management. Previously Mr. Knight was founding member of the joint technical committee of the Australia Standards and New Zealand Standards in charge of risk management[10].

In a conference, Kevin Knight stated that the AS/NZS 4360 was "due for update in 2009" and at the time "the most widely used global RM Standard" (Knight, 2009a, p. 2). The terms of reference for the working group nominated to develop the new standard were:

- To develop a document "which provides principles and practical guidance to the risk management process";

[10] Mr. Kevin Knight was invited to give contributions to the research process; his answers are included in the following chapters.

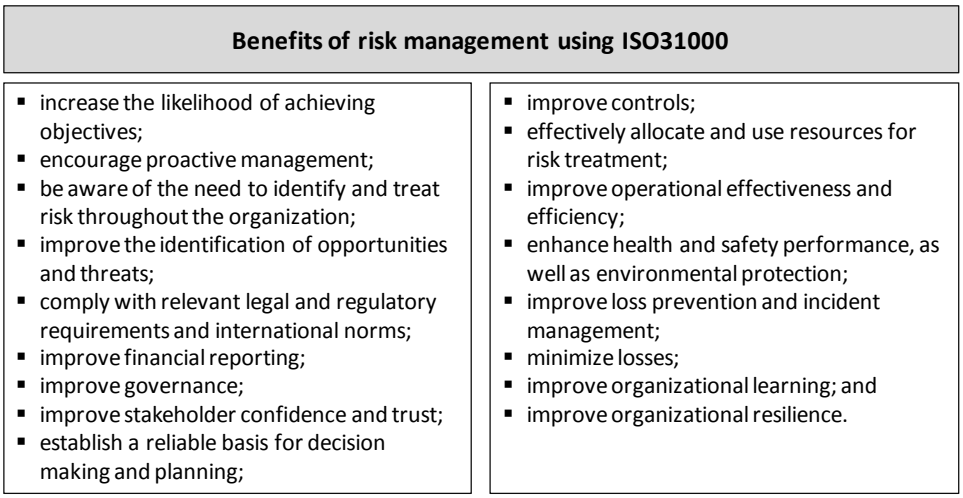
- To guarantee that the document "is applicable to all organisations, regardless of type, size, activities and location and should apply to all types of risk"; and
- To ensure the document establishes "a common concept of risk management process and common related concepts" (Knight, 2009a, p. 3).

Output of this effort should be a document that serves as guideline without certification purposes, therefore organisations that implement it can adapt and adjust according to their needs and requirements without being harmed as in other standardisation cases.

The ISO 31000 standard "recommends that organisations develop, implement and continuously improve a framework whose purpose is to integrate the process for managing risk into the organisation's overall governance, strategy and planning, management, reporting processes, policies, values and culture" (International Organisation for Standardisation, 2009a, p. v).

By implementing an ISO 31000-based risk management approach, the organisation can, among others, benefit from a better management with aligned strategy, fulfil all compliance-related requirements and improve its governance models. The figure below shows the complete list of benefits as mentioned in the standard.

Figure 49: Benefits of risk management using ISO 31000



Source: (International Organisation for Standardisation, 2009a, p. v)

In a handbook recently drafted by the Standards Australia and Standards New Zealand bodies[11], with risk management guidelines for implementing ISO 31000, the relationship

[11] This handbook ("DR HB 436 - Risk Management Guidelines, Companion to ISO 31000:2009; Draft for Public Comment") is at draft stage and, at the time of writing of this thesis (late 2013 – early 2014), object of public consultation for input and comment.

between ISO 31000:2009 and its precursor document AS/NZS 4360:2004 is explained: "there are important improvements that have resulted from the international collaboration and consultation that occurred in the development of the international standard – a standard that both Australia and New Zealand have adopted in place of AS/NZS 4360. Principal amongst these improvements are:

- Risk is now defined in terms of the effect of uncertainty on objectives.
- The principles that organisations need to follow to ensure they 'manage the risk associated with managing risk' have been made more explicit.
- There is much greater emphasis and guidance on how risk management should be implemented and integrated into organisations through continuous improvement of the framework that delivers both the mandate and capability to manage risk effectively" (Standards Australia / Standards New Zealand, 2013, p. 2).

It becomes therefore relevant to look into the core elements of the new ISO 31000:2009; the next section addresses these in a concise manner.

4.2.2. Core elements

As mentioned earlier, unlike other standards with negative or neutral definitions of risk, ISO 31000 presents a broad definition, considering positive and negative events as possible risk sources. Considering that risk is "the effect of uncertainty on objectives" (International Organisation for Standardisation, 2009a, p. 1) a number of different conclusions can be drawn from here:

- it is assumed that organisations have defined objectives, implying that these are based on thorough studies, planned for, decided upon and communicated to relevant stakeholders;
- that management actively steers the company towards the achievement of those objectives;
- that there are events that can have a number of different outcomes if and when they occur, regardless of how controllable those events are – even in the case of uncontrollable events, their consequences affect the organisation and these must be accounted for, too;
- that these outcomes can have positive, negative or even neutral impact on the organisation, for which it needs to be prepared with a portfolio of reactive, preventive or corrective controls;
- that (some of) the events and/or (some of) their outcomes can be controlled by the organisations' actions;
- the achievement of the organisations' objectives is therefore not a matter of luck or complete dependency on external issues, rather result of management preparedness to face the uncertainty related to such events.

Therefore companies are advised to introduce risk management practices that help them manage these events of uncertain outcomes. Risk management is defined as “coordinated activities to direct and control an organisation with regard to risk” (International Organisation for Standardisation, 2009a, p. 2).

By simplifying definitions and introducing flexibility to adjust the standard to the organisations’ needs, ISO 31000 is a tool that really helps organisations managing their business. It is based on three simple and clearly designed pillars: founding principles, overall framework and detailed process.

The 11 founding principles relate to the understanding of risk management, its contribution and importance in the organisation’s internal decision making processes. They are:

a) ”Risk management creates and protects value.
b) Risk management is an integral part of all organisational processes.
c) Risk management is part of decision making.
d) Risk management explicitly addresses uncertainty.
e) Risk management is systematic, structured and timely.
f) Risk management is based on the best available information.
g) Risk management is tailored.
h) Risk management takes human and cultural factors into account.
i) Risk management is transparent and inclusive.
j) Risk management is dynamic, iterative and responsive to change.
k) Risk management facilitates continual improvement of the organisation.” (International Organisation for Standardisation, 2009a, p. 8)

Despite being very clear, these principles also open the door to additional questions: for example in point f), if the best available information is incomplete, ambiguous or wrong, then any risk management effort based thereon will lead to equivalently bad decisions (this is true for any situation in the companies’ life and management process).

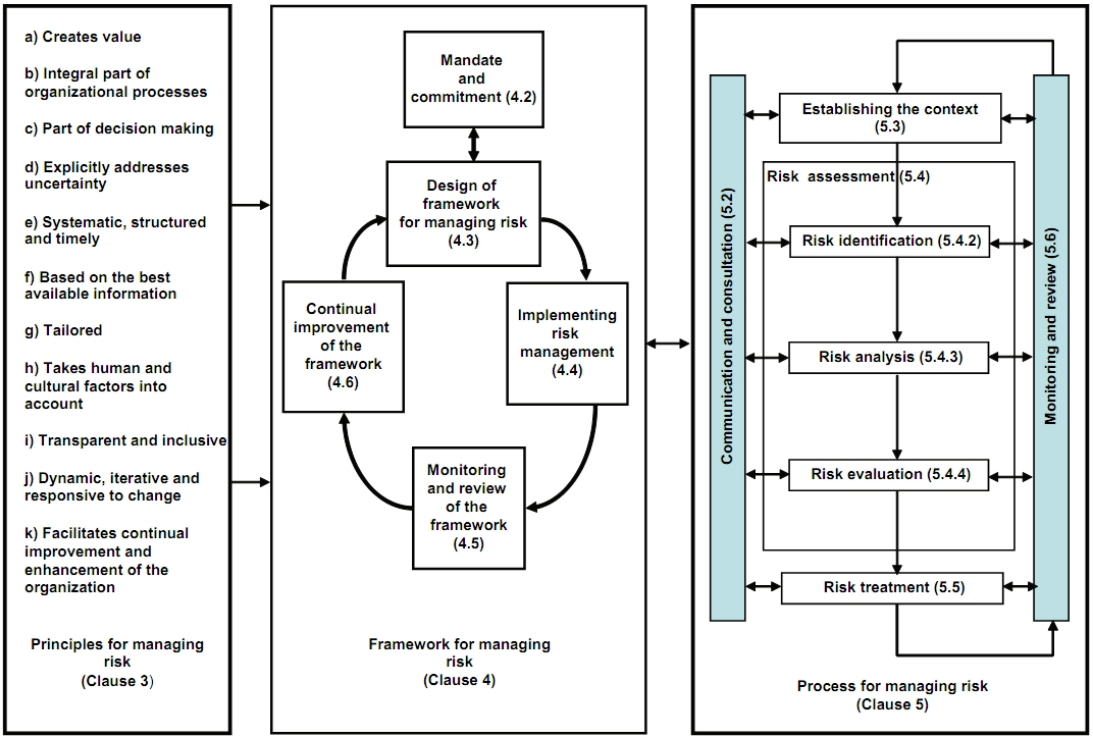
Based on these principles, ISO 31000 proposes a revolving framework for managing risk that is aimed at ensuring “that information about risk derived from these processes is adequately reported and used as a basis for decision making and accountability at all relevant organisational levels” (International Organisation for Standardisation, 2009b, p. 8). Moreover “this framework is not intended to prescribe a management system, but rather to assist the organisation to integrate risk management into its overall management system” (International Organisation for Standardisation, 2009a, p. 9). This leaves the door open for adjustments according to the organisations’ needs and its existing practices. The standard

suggests organisations should adapt the framework if and when needed, but also stresses that existing risk management practices should be critically reviewed against suggestions made by this standard, in order to "determine their adequacy and effectiveness".

This suggested framework has a starting element and then four additional revolving elements, as can be seen in Figure 50: Core elements of ISO 31000:

1. "Mandate and commitment", is linked to the definition of a clear mandate to the risk management unit by upper management, the need to align goals and objectives, corporate culture and risk management, as well as ensuring legal and regulatory compliance. Additionally this step intends to assign responsibilities, allocate resources, communicate to stakeholders and constantly review validity of the whole risk management framework.
2. "Design of framework for managing risk", relates to understanding the specificities of the organisation and its internal and external environment, as these can influence the risk management approach and framework. A subsequent task would be to design the organisations' risk management policy, duly signed by top management and communicated to all stakeholders. This policy should include the description of the companies' approach to risk, overall objectives of the risk management effort, who is responsible, how it is reported, etc. This way, the ownership and accountability for the whole process, and roles and responsibilities of individual risk owners become defined, enabling an easier handling and communication throughout the risk management process. Based thereon it becomes easier to identify resources required and allocate them to the task at hand, establish communication lines and reporting mechanisms.
3. The "Implementing risk management" element, involves the materialisation of the plans and decisions taken in previous elements. It's about applying the risk management policy and process, organise training and development sessions with involved staff, constantly communicate and consult with relevant internal and external stakeholders. As will be seen later, communication and consultation is a essential supporting activity that guarantees the success of the whole process.
4. "Monitoring and review of the framework" consists of measuring the performance of the designed risk management approach and the implementation thereof against predefined goals and indicators. This should be done periodically in order to identify potential shortcomings and corrective actions to the process itself.
5. Finally "continual improvement of the framework" assumes the results of the previous element and translates these into actual corrections and adjustments to the risk management process.

Figure 50: Core elements of ISO 31000



Source: (International Organisation for Standardisation, 2009a, p. vii);
Note: Numbers in brackets in the *Framework* and *Process* descriptions refer to text paragraphs in the ISO 31000 document. (4.1), missing from the graph, refers to *General* aspects in the actual *Framework* description.

Finally the standard shows how the process for managing risk should be structured. It is composed of seven steps that are in part sequential with two supporting activities:

1. "Communication and consultation" is considered to be essential throughout the whole process, therefore it gathers contributions and delivers input for all remaining steps. The ISO 31000 refers to a "consultative team approach" that helps implementing, managing, supporting and facilitating the whole process.
2. "Establishing the context" refers to the understanding of the social, economic, legal, technical, financial environment (among many other possible elements) the organisation is working in. It involves looking into the internal structure and external conditions, regulations and requirements in order to address, design or adjust the risk management process to the specificities of the organisation. Herein it is also relevant to define the criteria that will be used in the process to evaluate and assess each identified risk.
3. The "risk assessment: risk identification" step is the first step in the risk assessment stage. Several tools and techniques can be used to identify risk – these have been generically mentioned in a previous section of this thesis, the options suggested by ISO 31000 will be mentioned in the next section.
4. "Risk assessment: risk analysis" involves understanding each risk item, its root causes, direct and indirect consequences, attributes, etc. This looks into classifying the risk in terms of likelihood of occurrence and impact on the organisation, or

even further metrics to analyse the risk. If it is a quantifiable risk, a number of mathematical methods can be applied to support the decision making process. If not, qualitative analysis and judgement can replace the data-based approach.

5. "Risk assessment: risk evaluation" considers prioritising the risk against all other items, according to their impact and likelihood. Legal, regulatory, competitive, production or financial issues can contribute to the prioritisation process. Possible treatment actions can be identified and allocated, as well as related responsibilities and deadlines. "In some circumstances, the risk evaluation can lead to a decision to undertake further analysis. The risk evaluation can also lead to a decision not to treat the risk in any way other than maintaining existing controls. This decision will be influenced by the organisation's risk attitude and the risk criteria that have been established" (International Organisation for Standardisation, 2009a, p. 18).
6. "Risk treatment" is about implementing treatment options and control measures to mitigate the previously identified risks. This starts the cyclical process as the impact of a treated risk is expected to reduce, yet it still needs to be assessed, analysed and evaluated properly in order to understand if it is still relevant and what alternative treatment options are available. In some cases a risk cannot be further mitigated so that the organisation may end up accepting the exposure to that risk.
7. Monitoring and Review is the second overall supporting activity giving the whole process more substance. By providing the possibility to identify internal shortcomings, the process allows for self-correction and continuous improvement. This is aimed at ensuring the efficiency of the designed process, enabling corrections if and when needed.

4.2.3. Supporting documentation

The ISO 31000 standard has been released with two supporting documents: the "*IEC31010:2009 Risk Management – Risk assessment techniques*" published by the International Electrotechnical Commission and the International Organisation for Standardisation (International Organisation for Standardisation, 2009b); and the "ISO Guide 73:2009" (International Organisation for Standardisation, 2009c).

While Guide 73 contains all the vocabulary usable in a risk management framework, its definitions and guidelines for use in standards, IEC31010 is a more hands-on document with practical advice on how to apply ISO 31000. Guide 73 is a true dictionary and reference document covering concepts from risk and event to risk management process and risk universe. It is quite complete and thorough and helps organisations in using a common language, with the same understanding on different concepts, when implementing risk management.

IEC31010 provides templates and sample risk classification matrices with respective explanation of criteria and attributes used. Moreover it includes a brief description of more than 30 different quantitative and qualitative tools and techniques for use in the risk assessment process, with an indication of their applicability in the various stages of the risk assessment step. The figure below summarises all possible tools and their applicability.

Figure 51: Applicability of tools used for risk assessment

Tools and techniques	Risk assessment process					See Annex
	Risk Identification	Risk analysis			Risk evaluation	
		Consequence	Probability	Level of risk		
Brainstorming	SA[1)]	NA[2)]	NA	NA	NA	B 01
Structured or semi-structured interviews	SA	NA	NA	NA	NA	B 02
Delphi	SA	NA	NA	NA	NA	B 03
Check-lists	SA	NA	NA	NA	NA	B 04
Primary hazard analysis	SA	NA	NA	NA	NA	B 05
Hazard and operability studies (HAZOP)	SA	SA	A[3)]	A	A	B 06
Hazard Analysis and Critical Control Points (HACCP)	SA	SA	NA	NA	SA	B 07
Environmental risk assessment	SA	SA	SA	SA	SA	B 08
Structure « What if? » (SWIFT)	SA	SA	SA	SA	SA	B 09
Scenario analysis	SA	SA	A	A	A	B 10
Business impact analysis	A	SA	A	A	A	B 11
Root cause analysis	NA	SA	SA	SA	SA	B 12
Failure mode effect analysis	SA	SA	SA	SA	SA	B 13
Fault tree analysis	A	NA	SA	A	A	B 14
Event tree analysis	A	SA	A	A	NA	B 15
Cause and consequence analysis	A	SA	SA	A	A	B 16
Cause-and-effect analysis	SA	SA	NA	NA	NA	B 17
Layer protection analysis (LOPA)	A	SA	A	A	NA	B 18
Decision tree	NA	SA	SA	A	A	B 19
Human reliability analysis	SA	SA	SA	SA	A	B 20
Bow tie analysis	NA	A	SA	SA	A	B 21
Reliability centred maintenance	SA	SA	SA	SA	SA	B 22
Sneak circuit analysis	A	NA	NA	NA	NA	B 23
Markov analysis	A	SA	NA	NA	NA	B 24
Monte Carlo simulation	NA	NA	NA	NA	SA	B 25
Bayesian statistics and Bayes Nets	NA	SA	NA	NA	SA	B 26
FN curves	A	SA	SA	A	SA	B 27
Risk indices	A	SA	SA	A	SA	B 28
Consequence/probability matrix	SA	SA	SA	SA	A	B 29
Cost/benefit analysis	A	SA	A	A	A	B 30
Multi-criteria decision analysis (MCDA)	A	SA	A	SA	A	B 31

[1)] Strongly applicable.
[2)] Not applicable.
[3)] Applicable.

Source: (International Organisation for Standardisation, 2009b, p. 22); Note: Annexes referenced to in the last column of the table are contained in the original ISO 31000:2009 document

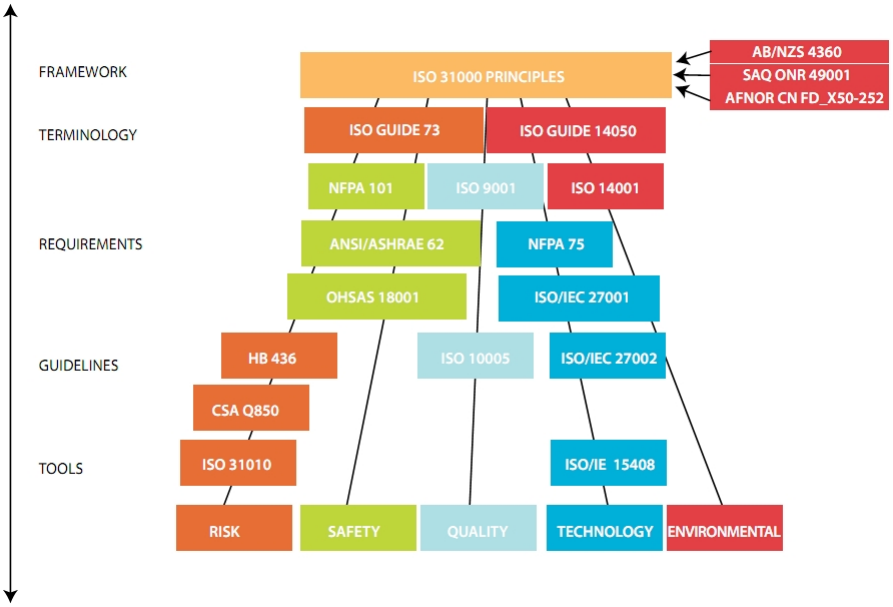
Additionally, as mentioned in a previous section, a third supporting document is being prepared by the Risk Management Committee OB-007 of the Australian Standards and New Zealand Standards organisations. It is the draft version of "DR HB 436 – Risk Management Guidelines, Companion to AS/NZS ISO 31000:2009" currently in a public consultation process. It takes the implementation support one step further by explaining:

- "How to use the eleven principles of effective risk (...).
- How to either set up or enhance the organisation's existing framework for managing risk so as to express the intent and acquire the capability to manage risk more effectively.
- How to establish the context and then, based on this, identify, analyse, evaluate and, where warranted, treat risk. To support these processes, the Handbook explains how to communicate with and consult stakeholders and how to use monitoring and review techniques to ensure ongoing effectiveness and assimilate change."
  (Standards Australia / Standards New Zealand, 2013, p. 7)

4.2.4. Integration with other ISO standards

The ISO 31000 standard has not been produced for certification purposes, being therefore different from some other ISO standards like the ISO9000 on Quality Management, the ISO14000 on Environmental Management or the ISO26000 on Social Responsibility. It is still interesting to see how the various standards produced by the International Organisation for Standardisation are linked to each other. A comparison paper produced by RIMS shows a figure, depicted below, that helps getting a feeling of how ISO 31000 relates to some of those other standards.

Figure 52: A selection of standards



Source: (RIMS, 2011, p. 22)

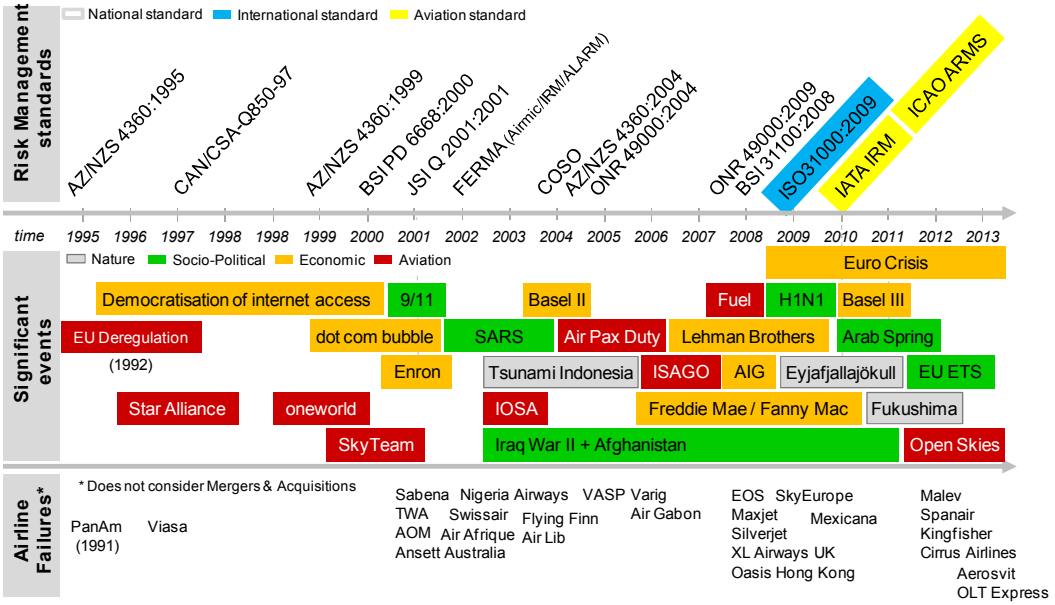
The principles and terminology underlying the ISO 31000 are drawn from Guide 73 and Guide 14050. On the other hand, the principles used by ISO 31000 also gather input from the national risk management standards AZ/NZS4360 (Australia / New Zealand), ONR 490001 (Austria) and AFNOR CN FD_Z50-252 (France). All respective guidelines and tools are then aligned with the respective core subject of the standard: risk, safety, quality, technology or environment.

RIMS states “using standards may be a proactive way to protect brand and reputation, in addition to providing a defensible position. The bottom line benefit for using standards is that (...) their use can make your organisation more resilient in the face of emerging risks and adverse events” (RIMS, 2011, p. 22).

4.3. Aviation specific risk management frameworks

While national organisations were drafting their risk management standards, and the International Organisation for Standardisation was designing its own approach, two aviation-specific bodies were also working on their own frameworks for risk management. The International Air Transport Association, an international association representing some of the largest airlines in the world, produced their *Integrated Risk Management Guidance Manual* in 2010 (IATA, 2010). The International Civil Aviation Organisation, an international institution comprehending most nations, published their *Operational Risk Assessment in Aviation Organisations*, also in 2010, as result of the work conducted by the Aviation Risk Management Solutions Group between 2007 and 2010 (ICAO, 2010).

Figure 53: Risk Management standards in the aviation context



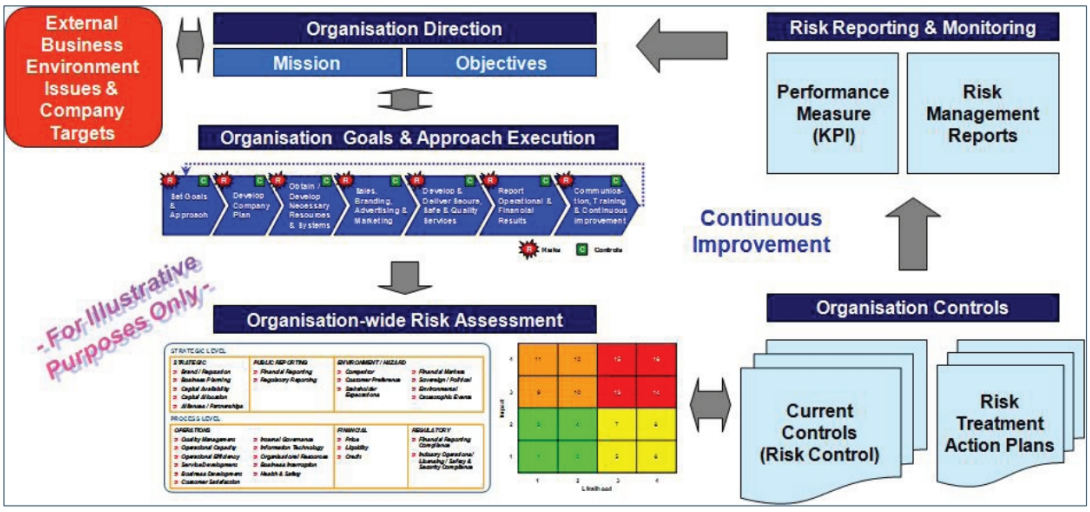
Over time, the number of risks, their nature and geographical reach has increased tremendously, coupled with the more integrated and interdependent character of air transport in the global economy. While risk management is supposed to help companies better manage their business and ultimately help them achieving and/or improving profitability, it can be seen that the availability of risk management standards (regardless of national, international or aviation specific) did not avoid airlines from failing. The sheer availability of such standards is of course no guarantee that airline organisations are using them or that, when so, they are being used properly. A review of current risk management practices at airlines is reserved for the next chapter, while the present section will be dedicated to outlining the two airline-specific risk management models mentioned above.

4.3.1. IATA's Integrated Risk Management

As international body representing and serving the airline community, the International Air Transport Association produces a number of guidelines and standards to be used by member and non-member airlines. Over the last decade, the launch of IOSA (the IATA Operational Safety Audit), of ISAGO (the IATA Safety Audit for Ground Operations) as well as the AHM (Airport Handling Manual) have all been asking airlines to demonstrate how they were performing risk management in the respective fields of their business. As this was looking mostly into broad operational issues, IATA decided to launch a Guidance Manual for their Integrated Risk Management (IRM) in 2010. Therein IATA states that the IRM is a follow up to IATA's Integrated Aviation Management System previously published in 2007 and that "it is tailored for the aviation industry with an emphasis on operations across the organisation" (IATA, 2010, p. 7).

This is a revolving framework with no clear starting or ending point. Core elements are the organisations' direction and goals, the organisations' risk assessment, organisational controls and the risk reporting and monitoring. The below picture summarises the proposed framework.

Figure 54: IATA Risk Management Framework



Source: (IATA, 2010, p. 19)

According to IATA's Guidance Manual, the process starts with a self-assessment checklist whose key components are (IATA, 2010, p. 7):

a) A risk management framework, that establishes the basics of the process and the link to the organisations' strategy and goals;
b) A methodology, with a customised model, risk rating parameters, clear process steps and a comprehensive risk register;
c) An oversight structure and terms of reference, indicating who is ultimately responsible for the process and each individual risks;
d) Policy and guidelines, as reference document for implementation purposes;
e) Risk management awareness, communication and training, to spread the understanding of and create a risk management culture within the organisation;
f) Performance measures or indicators that will be used to track the effectiveness and success of the whole process.

It is unclear how this self-assessment fits into the overall framework proposed by IATA.

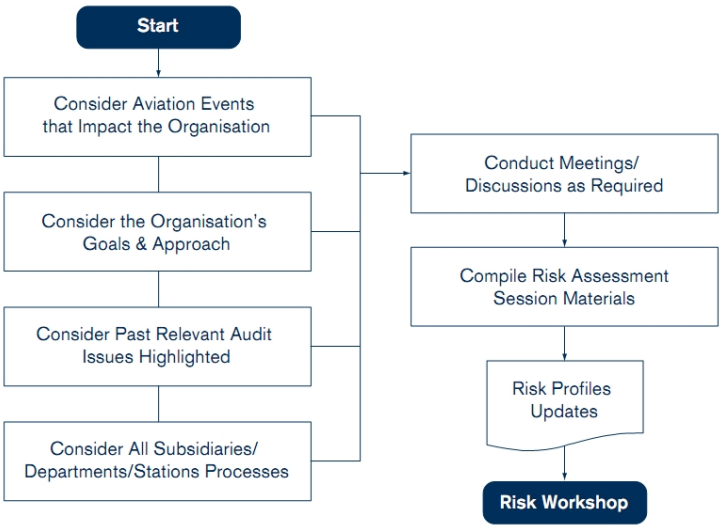
Moreover, the manual states: "Once the organisation has completed the IRM Self Assessment Checklist, the checklist can be returned to IATA. At the option of the organisation, the following can be carried out: a) obtain IATA's services to carry out a high level validation of the information updated in the checklist – once the validation has been completed, high level advice can be provided (...) or b) Should additional assistance be required to implement a more robust risk management process, consultancy services can be obtained from IATA" (IATA, 2010, p. 9). It is unclear if the whole process has been designed to help the airlines in managing their risk or to serve as additional platform for IATA to distribute its services.

Further on, the manual compares the IATA IRM Technique against industry Risk Management Requirements as outlined by IOSA, ISAGO and AHM documentation. While these are true industry-specific elements, risk management is by definition industry-neutral and risks can arise from non-industry specific sources. By focussing only on safety and operations, the proposed risk identification process is therefore flawed and incomplete from the start.

As can be seen in Figure 55: IATA's IRM Risk Identification Process, the proposed risk assessment process starts by considering aviation events that can impact the organisation. It seems to exclude all other events and risk sources that are beyond the aviation business but could have an impact on it. In this process, a "simple question" asked is "what events/items/occurrences/processes can go wrong?" (IATA, 2010, p. 20), leading to the

conclusion that the underlying risk definition has a negative nature. Actually, when it comes to defining risk, this manual states that risk is “the potential for an event (internal or external) resulting in adverse financial, operational or other impact” (IATA, 2010, p. 4).

Figure 55: IATA’s IRM Risk Identification Process



Source: (IATA, 2010, p. 20)

Further on the manual proposes a customized risk model that has been “tailored specifically for the aviation industry”, although it suggests it is a sample that should be customized by each organisation willing to implement a risk management process. By analysing this “customised model”, none of the contained elements are unique and specific to the aviation industry.

Figure 56: IATA’s IRM Sample Risk Model Customised for the Aviation Industry

Source: (IATA, 2010, p. 22)

The manual makes only minor references to other industry-neutral risk management standards available at the time of its production, as it considers risk management part of corporate governance codes airlines can choose to comply with.

Interestingly, in an interview conducted with IATA's Director Risk and Insurance Management, the main statement was that it has been difficult to convey the message of the importance of risk management to airlines, its benefits and the value of the proposed process. The manual quotes implementations for two Egyptian ground handling organisations in 2010, but there is no evidence of further implementations since then at airlines or any other related businesses.

IATA's working group on Risk Management and Insurance seems to be hermetic, as requests for comment were rejected. No airline risk manager interviewed during the field work process (see next chapter) was involved with this working group, either.

Moreover, a special report on risk management contained in the December 2012 edition of *Airlines International*, IATA's flagship magazine to publicly communicate with the industry and interested stakeholders, does not even refer to IATA's IRM Technique. It makes strong references to safety and insurance, quoting the success of the IOSA program when it comes to preventing accidents. "Figures for 2011 prove the rarity of such an event. Last year was the safest year ever for air transport. The accident rate (measured in hull losses per million flights of Western-built jets) was 0.37. Airlines registered with the IATA Operational Safety Audit (IOSA) clearly benefited from global standards; their overall accident rate was 52% better than for non-IOSA operators" (IATA, 2012c, p. 1). The article moves on to the importance of insurance and having good relationships with the insurance community and related business partners. This was of course a missed opportunity to expose and promote risk management in a truly integrated way, as seems desired by the IRM Guidance Manual.

When looking at IATA's homepage, the IRM Guidance Manual is not shown on the "Standards, Manuals and Guidelines" quick-links, and only appears in a secondary page classified as a legal document, being available for purchase.

While it is positive that IATA proposed an industry-specific risk management framework, it is complex in content and graphical depiction, it over complicates a process that should be simple and understandable, given the complexity of the risk management topic itself.

4.3.2. ICAO's Operational Risk Assessment

The International Civil Aviation Organisation, a United Nations specialised agency that promotes aviation safety by setting standards for safety, security, efficiency, regularity and environmental protection, issued in 2010 an Operational Risk Assessment methodology in Aviation Organisations (ICAO, 2010). This comes as consequence and complement of the Safety Management Systems Manual published by ICAO where its chapters 5 and 9 call for the need of risk management in the context of Safety Management Systems. Therefore, ICAO's Aviation Risk Management Solutions Working Group gathered during 2007-2010 input from several organisations to produce the aforementioned document. Members of this group include mostly airline representatives, although manufacturers, academics, service providers, research centres and consultants were also present. The group was open to receive people with practical experience, willing to contribute for the development of such a new document. No IATA representative is listed as member of this working group.

The document provides the risk definition proposed by Douglas Hubbard that also has a negative connotation to it: "Risk is a state of uncertainty where some of the possibilities involve a loss, catastrophe, or other undesirable outcome" (ICAO, 2010, p. 8). Unsurprisingly, the focus of the entire document is on safety and operational risks, despite mentioning the full array of possible risks: from financial and environmental, to reputation and security risks. It is clearly stated that "the ARMS methodology has been developed for Flight Safety risks" (ICAO, 2010, p. 11).

The document also distinguishes between the objectives of *risk management* and of *operational risk assessment* (ICAO, 2010, p. 7) as closely linked concepts:

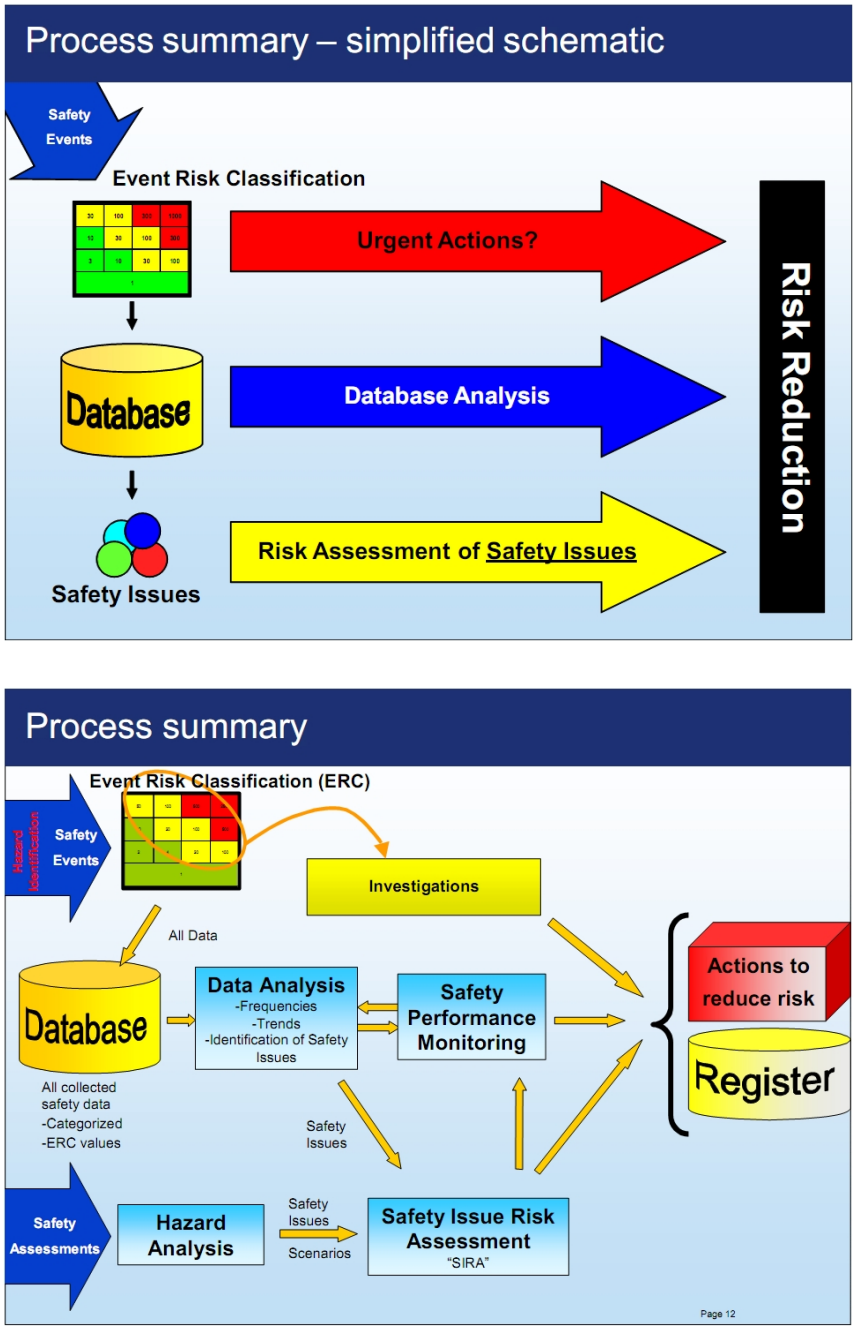
- "The main objective of Risk Management is to make sure that all risks remain at an acceptable level.
- The objective for Operational Risk Assessment (ORA) is the assessment of operational risks in a systematic, robust and intellectually cohesive manner"

Therefore Operational Risk Assessment is about the identification, assessment, evaluation and treatment of those operational risks, "consisting of three elements: hazard identification, risk assessment and risk reduction (mitigation in ICAO terminology)", while risk management refers to the whole process.

To achieve this, ICAO's Operational Risk Assessment is built around two blocks: the Event Risk Classification (ERC) and the Safety Issue Risk Assessment (SIRA). While ERC is the first

step in the process, it basically aims at understanding each event and classifying it according to preformatted parameters. SIRA is used for safety issues. Herein is an important distinction to be made: *event* versus *issues*, as not every event can become a safety issue. The simplistic schematic presented below makes it more transparent, especially when complemented by the complete process flowchart.

Figure 57: ICAO ARMS Process – simplified schematics and complete flowchart



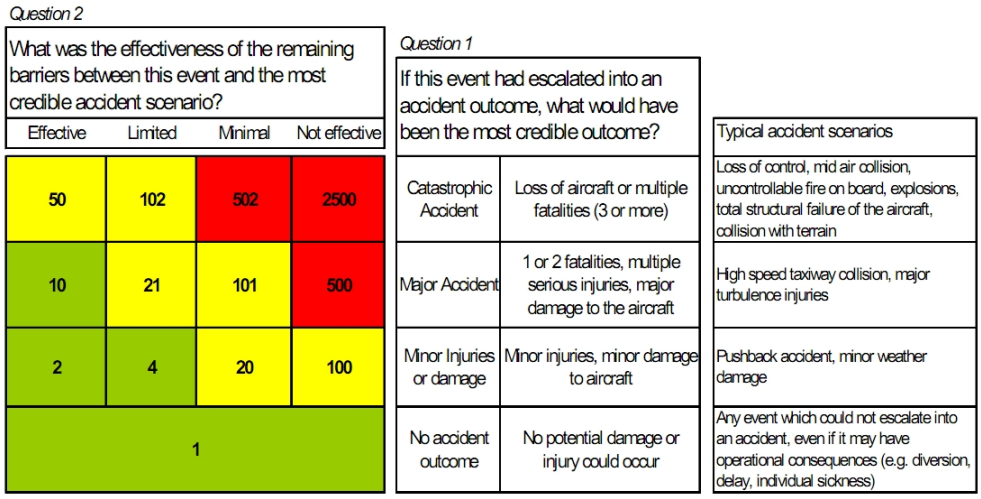
Source: (ICAO, 2010)

It is clear that the first step is the ERC using a two-dimensional matrix to classify each event. For this classification, the methodology suggests answering two questions:

1. "If this event had escalated into an accident, what would have been the most credible accident outcome?" providing four different answer options, from 'no accident outcome' to 'catastrophic accident'; and
2. "What was the effectiveness of the remaining barriers between this event and the most credible accident outcome?" also providing four options, from 'effective' to not effective.

The result is a heat map that contains a depiction of each event, in green being those that don't require additional corrective actions, in yellow those that require further investigation and a more refined risk assessment and in red the events that require immediate action and investigation.

Figure 58: ICAO ARMS Event Risk Classification



Source: (ICAO, 2010)

All events feed the database, providing information for future risk assessments and safety performance monitoring exercises. Those events that have an impact on safety and require further investigation move on to the second building block of the ARMS Methodology, the Safety Issue Risk Assessment.

Herein, ICAO suggests starting by describing the issue comprehensively and splitting it into sub-issues, if possible. This allows for a better analysis of the major issue, separating possible causes and respective mitigation actions.

The issue is to be assessed “using a formula where risk has four factors:

1. Frequency/probability of the so-called Triggering Event,
2. Effectiveness of the Avoidance Barriers,
3. Effectiveness of the Recovery Barriers ,
4. Severity of the (most probable) accident outcome.”
   (ICAO, 2010, p. 27)

To support this process, ICAO published an excel-spreadsheet that can be used as template. Moreover the ARMS Methodology document provides extensive guidance in form of examples and template tables that can be used for this analysis step.

While initially developed for airlines, ICAO suggests a number of customisation possibilities for organisations without flight operations such as ground handling or maintenance organisations; for large and small aircraft operators; and also enables the customisation of the risk matrices. A one-page quick user guide is also provided as a day-to-day help for those using this approach frequently.

While this approach seems simple to understand and easy to implement, it is only applicable to safety related events. All other ones, notably those related to the management of the airline business, are not covered.

4.4. Chapter Summary: filtering all options to select one guiding standard

This chapter summarised the various industry-neutral and industry-specific risk management standards published over the recent years. The link to national and international corporate governance guidelines has been established, showing that risk management is becoming a requirement for proper governance. Nevertheless, none of these corporate governance guidelines recommend the use of one particular risk management standard, leaving it to each organization to choose the one it finds most suitable.

It has also been shown that most risk management standards are either incomplete or from its inception directed to one industry (as is the case with SOLVENCY II). Very few of these standards have broad risk definitions, considering only the negative aspects of events as risks. This, coupled with the lack of a proper root cause analysis as well as missing guidelines for business resiliency and sustainability, lead to an exclusion of COSO (as strongest contender) when compared to the more recent and international ISO 31000.

ISO 31000 has thus been considered the most widely applicable risk management standard and chosen as guideline for further developments in this thesis.

As for the two industry-specific risk management standards produced by IATA and ICAO, none is truly holistic (ICAO) or easy to implement (IATA). Given the limited adherence by the airline community to implement these, notably the IATA IRM, this organisation seems to have failed in their endeavour to bring holistic risk management closer to the airline industry. It is necessary to understand why this happens, since IATA is the leading global airline body successfully setting standards in so many fields. Internal bureaucracy, lack of leadership, goals and guidance, or even limited airline involvement in the development of this standard may be part of the explanation.

Nevertheless, as with IATA's IOSA, ISAGO and AHM suggestions, ICAO's ARMS Methodology proves that operational areas are already well covered in an airlines' operation. The major shortcoming is the business related aspect, which seems to be deficiently covered. Very rarely have airlines failed[12] because of operational occurrences; the opposite is true for business-related mismanagement, wrong financial, strategic and business planning, and misaligned strategic goals and direction. Recalling Figure 53 above, none of the airline failures mentioned were due to safety related issues, rather all due to financial distress, competitive pressures, wrong strategic choices or utter mismanagement. It becomes therefore necessary to understand if and how airlines are currently managing all their risks: if they are only looking at the operational ones (which they have to, given strict regulatory requirements) or if they use more overwhelming and all-encompassing approaches based on any of the above mentioned risk management models and standards. This will be covered in the next chapter.

[12] Failure is understood as leading to the complete bankruptcy of the airline.

– Intentionally left blank –

5. Current Risk Management practices at airlines

What are typical airline risks? How do airlines identify them? What processes do they use to manage risks? Are these processes inspired on any existing standard or do airlines use their own in-house developed approaches? How does the use of risk management influence the financial performance of airlines? And can such a link be established?

Lots of questions arise when it comes to understanding what the current risk management practices are at airlines worldwide. This is the core chapter of this thesis on which most information gathered from field work was concentrated. Chapter 3 detailed the methodological aspects of this research process, focussing on desk research, interviews, survey and other supporting activities. This chapter will comprehensively address the results of these working packages, as an attempt to answer all questions.

5.1. Global airline risk factors

In an article published in the April 2002 edition of the Airline Business magazine, Michael Zea (at the time consultant at Mercer Management Consulting) exposed his views on how airlines were and should be managing risk originating from a number of identified events. His analysis consisted of mapping out 45 risk factors that traditionally affected airlines, in an attempt to understand how airlines were managing them. He concluded that:

- “Nearly two-thirds could have been avoided using available risk management techniques.
- Ten of the events could have been mitigated through traditional means, such as insurance or financial derivatives.
- Some 14 could have been mitigated by more consistent and in-depth customer analysis, combined with scenario planning and game theory exercises.
- Finally, an additional eight events could have been mitigated through improved merger integration planning and improved execution.” (Zea, 2002, p. 3)

Nevertheless, he suggests that the traditional approach was to “see risk management in terms of hazards, such as the need to protect physical assets”, therefore contracting insurance policies to cover such material losses. Unsurprisingly, most of those 45 risk factors were not properly covered. Michael Zea stresses that holistic risk management efforts ought to be comprehensive “aligning people, processes and technology to maximise enterprise value”, because “not all risks are material (...); individual risks should be evaluated on a portfolio basis to understand and appreciate correlations among risks; and

risk management is an ongoing process, not a one-time event", such as a material loss that can be covered by an insurance policy (Zea, 2002, p. 1).

His analysis maps out risk events in a landscape (see Figure 59) that resembles the one presented in Figure 23 – Industry Portfolio of Risk, shown in an earlier chapter. This depiction shows risks split among two natures (internal and external) and four types:

1. Strategic risks, understood as related to global choices made by the companies' management. Examples include 'market share battles', 'corporate culture' and 'alliances/code-sharing troubles'.
2. Operational risks, related to the technical aspect of the airline operation, including 'maintenance/reliability' issues, 'network constraints' or 'major IROP's' (Irregular Operations)
3. Financial risks, covering capital and cash management issues, such as 'aircraft acquisition' decisions, 'fuel prices' development and their impact on the airlines' profitability, or 'credit rating' impacting the airlines' access to credit facilities and their respective costs.
4. Hazard risks, for all other unclassifiable risk events such as 'weather', 'political risks' or '3rd party liability'.

Unquestionable focus and priority is given to the safety of the operation, at the core of this landscape. In fact, no airline will ever state that safety is not their primary concern, regardless of their actual safety record.

Figure 59: Airline Risk Factors

Source: (Zea, 2002, p. 2)

This was back in 2002. Given the further development of management and business administration theories, tools and methodologies, it is expectable that airlines modernised their risk management policies and changed towards a more integrated, holistic or enterprise risk management model.

The same Airline Business magazine, now in cooperation with AON, an airline insurance broker, launched in 2005 the Airline Risk Management Survey with a repeat edition in 2007. Roughly 50 airlines answered to the provided questionnaires, showing that risk management was far from being integrated, holistic or enterprise-wide.

While in 2007 86% of the respondents (67% in 2005) stated their companies had a company-wide risk management strategy, contracting insurances still seemed to be the primary solution to manage risks. 69% of all respondents said that insurance costs covered more than 50% of their risk management expenses (although down from 70% in 2005).

Figure 60: Airline Business Survey 2007 – broad areas covered by airlines' risk management strategy

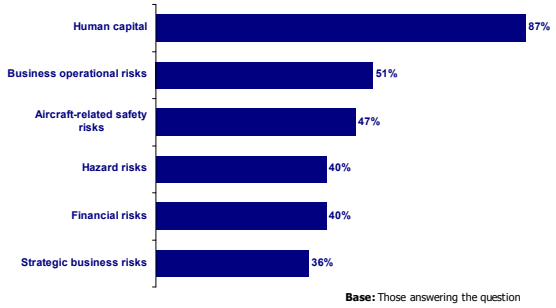
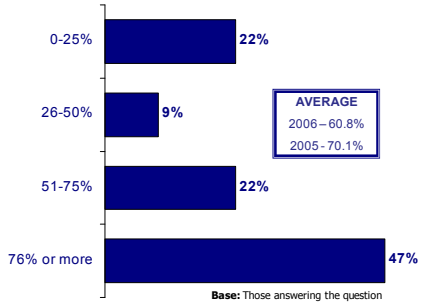


Figure 61: Airline Business Survey 2007 – insurance premium as percentage of total risk management expense



Source: (Airline Business, 2007, p. 13; 16)

At the same time, the main areas covered by the airlines' risk management were:

- 'Human capital' as main focus for 87% of respondents (up from 76% in 2005); of these 97% insure against employee accidents, 78% against personal accidents, 74% against workers compensation, 74% medical insurance, 72% life insurance and 62% long term disability cover;
- 'Business operational risks' for 51% of the respondents (down from 69% in 2005), including hazard and financial risks; and
- 'Aircraft related safety risks' for 47% of the respondents (down from 94% in 2005).

In this survey, 68% of responding airlines did not actively monitor the total cost of insurable risk and when asked about the organisations' attitude towards risk, 18% tend to transfer as

much as possible (down from 20% in 2005), 74% are comfortable in retaining some level of risk (68% in 2005), 4% are comfortable in retaining a high level of risk (8%) and 4% retain all but catastrophic risks (same in 2005). Risk retention methods included mostly corporate deductibles (86%), captive insurances company (41%), local deductibles (32%).

In terms of areas insured, aircraft accidents, war and terrorism, property damage and employee accidents are the most listed insurance reasons.

Figure 62: Airline Business Survey 2007 – Which of the following does your organisation currently insure against?

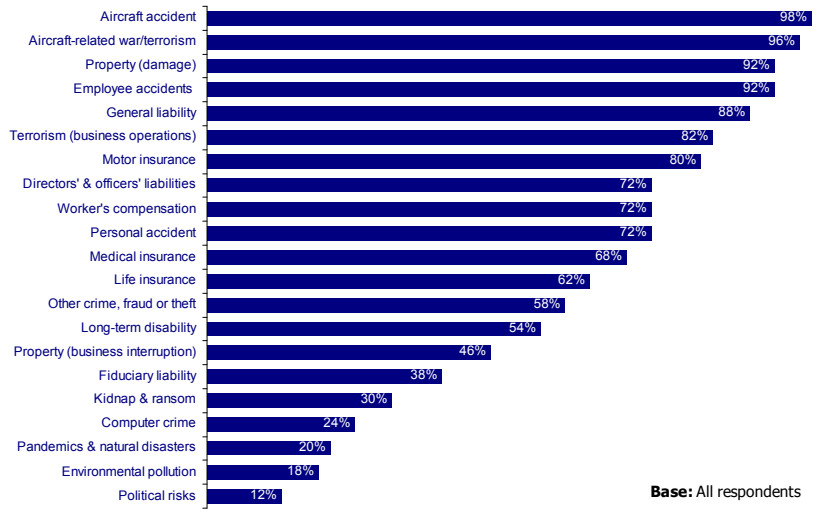
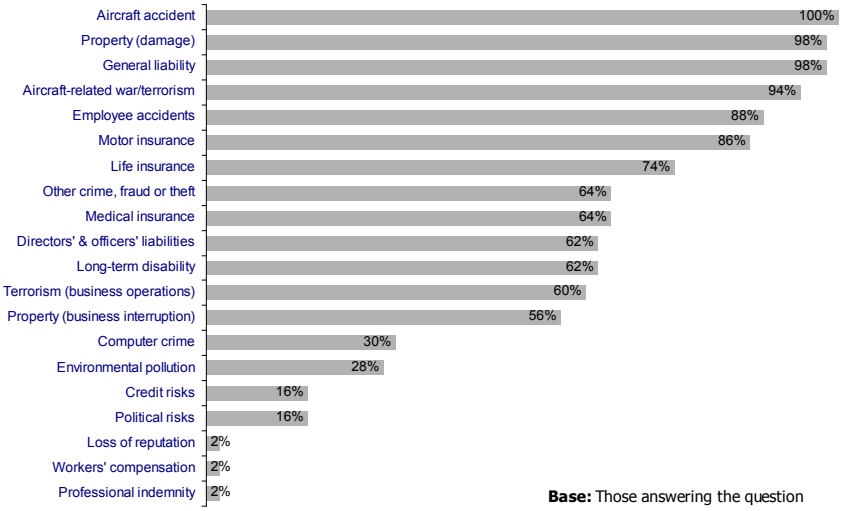


Figure 63: Airline Business Survey 2005 – Which of the following does your organisation currently insure against?



Source: (Airline Business, 2007, p. 26) and (Airline Business, 2005, p. 25)

These surveys show, of course, more results on the efficiency of insurance policies, market offerings, future challenges, achieved organisational successes and major failures – yet mostly with the focus of risk management as handled by insurances only. As seen above, airlines are affected by a number of risks, a few of them not at all insurable. In these surveys, there is no statement on risk management processes, organisation or standards used. While they are useful for the insurance business, they offer no holistic view and are already outdated since no updated version has been released since 2007.

This stresses the need for another review that, for the purposes of this research, focuses on the missing issues: use of risk management processes, organisation, standards, etc., more than focussing on use and cost of insurance policies.

5.2. Top 100 airlines survey results

Given the need to have an updated view of how airlines manage their risks, one key element of this thesis' field work is a survey conducted to the 100 largest airlines, measured by revenue. The initial goal was to have questionnaires sent out to risk managers or equivalent functions within those airlines, yet the lack of a suitable contact database forced a change in the desired approach. The next sections outline the methodological aspects of this work, followed by the analysis of quantitative and qualitative results achieved.

5.2.1. Methodological aspects

The main objectives were to understand what were the main risks affecting airlines and how they managed those risks. To achieve this purpose a survey was designed to analyse the latest available annual reports, corporate governance reports or social responsibility reports published by these airlines. Questions included the assessment of, among others:

- If and how risk management is handled in any or all of these reports;
- How much volume and in what depth risk management is covered;
- What organisational aspects on risk management are reported, notably ownership, task allocation, reporting and ultimate responsibility;
- The references to any specific risk management standard;
- The availability of a separate and freely accessible risk management policy;
- What risks are mentioned in these reports;
- And if there is any link between the use of any risk management standard and the financial performance achieved by these airlines.

The source of information was always the airlines' own annual reports, corporate governance and social sustainability as published on their websites, taking into account their latest available versions. In most cases, given the date this survey was conducted (late 2012, early 2013), these reports refer to the year 2011. Whenever 2012 versions were already available, information was completed if, where and when appropriate.

As mentioned, the survey covered the 100 largest airline groups, measured by revenue, as published in the 2012 World Airline Rankings of the Airline Business magazine in its August 2012 edition (Airline Business, 2012). These represent roughly 70% of the global airline revenues generated in 2011, considering a total of US $598 billion as published by IATA's 2012 Annual Review document (IATA, 2012a). This list includes the largest passenger and cargo airlines, from all regions in the world. The next table presents all included airlines.

Table 1: Top 100 airline groups included in the survey

Ranking 2011	Ranking 2010	Group/Airline	Country	Revenues $ million
1	(1)	**Lufthansa Group**	Germany	40.164
2	(2)	**United Continental Holdings**	United States	37.110
3	(3)	**Delta Air Lines**	United States	35.115
4	(4)	**Air France-KLM Group**	France	34.109
5	(5)	**FedEx**	United States	26.515
6	(6)	**AMR Corporation**	United States	23.979
7	(7)	**International Airlines Group**	United Kingdom	22.839
8	(9)	**ANA Group**	Japan	17.897
9	(10)	**Emirates**	United Arab Emirates	16.958
10	(14)	**Southwest Airlines**	United States	15.658
11	(8)	**Japan Airlines Group**	Japan	15.276
12	(11)	**Air China**	China	15.260
13	(13)	**Qantas**	Australia	14.842
14	(16)	**China Southern Airlines Group**	China	14.017
15	(12)	**US Airways**	United States	13.341
16	(17)	**China Eastern Airlines**	China	12.943
17	(15)	**Cathay Pacific Group**	Hong Kong	12.649
18	(18)	**Singapore Airlines Group**	Singapore	11.896
19	(19)	**Air Canada**	Canada	11.779
20	(20)	**Korean Air**	South Korea	10.676
21	(21)	**TAM Linhas Aereas**	Brazil	7.574
22	(24)	**Turkish Airlines (THY)**	Turkey	7.008
23	(25)	**Qatar Airways Group**	Qatar	6.825
24	(22)	**SAS Group**	Sweden	6.441
25	(23)	**Thai Airways International**	Thailand	6.361
26	(29)	**Ryanair**	Ireland	6.063
27	(28)	**UPS Airlines**	United States	5.941
28	(27)	**Air Berlin**	Germany	5.909
29	(31)	**LAN Airlines**	Chile	5.718
30	(30)	**EasyJet**	United Kingdom	5.552
31	(26)	**Saudia***	Saudi Arabia	5.500
32	(34)	**Aeroflot Russian Airlines**	Russia	5.388
33	(35)	**Alitalia**	Italy	4.862
34	(33)	**Asiana Airlines**	South Korea	4.821
35	(36)	**Malaysia Airlines**	Malaysia	4.549
36	(38)	**GOL Linhas Aereas Inteligentes**	Brazil	4.515
37	(40)	**JetBlue Airways**	United States	4.509
38	(32)	**China Airlines**	Taiwan	4.493
39	(37)	**Virgin Group***	United Kingdom	4.400
40	(39)	**Alaska Air Group**	United States	4.318
41	(47)	**Etihad Airways**	United Arab Emirates	4.100
42	(42)	**Hainan Airlines Group**	China	4.074
43	(45)	**AviancaTaca**	Colombia	3.815
44	(50)	**SkyWest Airlines****	United States	3.655
45	(41)	**EVA Air**	Taiwan	3.472
46	(48)	**Air New Zealand**	New Zealand	3.315
47	(53)	**Virgin Australia**	Australia	3.260
48	(44)	**Air India***	India	3.250
49	(46)	**TAP Portugal**	Portugal	3.215
50	(43)	**South African Airways***	South Africa	3.200
51	(49)	**Jet Airways**	India	3.157
52	(54)	**WestJet Airlines**	Canada	3.116
53	(58)	**Garuda Indonesia**	Indonesia	3.091
54	(52)	**Thomson Airways**	United Kingdom	2.983
55	(59)	**Transaero Airlines**	Russia	2.948
56	(57)	**Aeromexico**	Mexico	2.872
57	(51)	**Republic Airways Holdings**	United States	2.865
58	(55)	**Finnair**	Finland	2.757
59	(56)	**Air Transat**	Canada	2.619
60	(61)	**Vietnam Airlines***	Vietnam	2.200
61	(60)	**El Al**	Israel	2.043
62	(73)	**Norwegian**	Norway	1.892
63	(63)	**Cargolux**	Luxembourg	1.867
64	(75)	**UTair Aviation**	Russia	1.845
65	(68)	**Air Europa**	Spain	1.830
66	(74)	**Copa Airlines**	Panama	1.830
67	(69)	**Condor**	Germany	1.802
68	(66)	**Aer Lingus**	Ireland	1.801
69	(64)	**Volga-Dnepr Airlines**	Russia	1.752
70	(65)	**Philippine Airlines**	Philippines	1.712
71	(71)	**Jazz**	Canada	1.688
72	(76)	**Hawaiian Airlines**	United States	1.651
73	(70)	**Royal Air Maroc**	Morocco	1.607
74	(77)	**S7 Airlines**	Russia	1.543
75	(78)	**Ethiopian Airlines**	Ethiopia	1.517
76	(67)	**Thomas Cook Airlines (UK)***	United Kingdom	1.500
77	(62)	**Egyptair**	Egypt	1.500
78	(84)	**Shandong Airlines**	China	1.499
79	(81)	**AirAsia**	Malaysia	1.464
80	(82)	**Brussels Airlines**	Belgium	1.449
81	(79)	**Pakistan International Airlines**	Pakistan	1.345
82	(86)	**Kalitta Air**	United States	1.286
83	(80)	**Atlas Air**	United States	1.285
84	(90)	**Pinnacle Airlines**	United States	1.232
85	(87)	**Kenya Airways**	Kenya	1.213
86	(88)	**Vueling Airlines**	Spain	1.207
87	(83)	**Aerolineas Argentinas***	Argentina	1.200
88	(96)	**IndiGo***	India	1.200
89	(72)	**Kingfisher Airlines**	India	1.189
90	(102)	**Spirit Airlines**	United States	1.071
91	(92)	**LOT Polish Airlines**	Poland	1.065
92	(89)	**Nippon Cargo Airlines**	Japan	1.049
93	(93)	**Royal Jordanian Airlines**	Jordan	1.038
94	(106)	**Virgin America**	United States	1.037
95	(111)	**Skymark Airlines**	Japan	1.018
96	(85)	**Gulf Air***	Bahrain	1.000
96		**Lion Air***	Indonesia	1.000
98	(95)	**Flybe**	United Kingdom	987
99	(100)	**WIZZ Air***	Hungary	950
100	(94)	**Monarch Airlines***	United Kingdom	950

Source: (Airline Business, 2012, p. 44); Note: airlines marked with asterisk refer to those where full year revenue figures were unavailable; the source made estimates to give an indication of the airlines' ranking.

There are of course a number of limitations that can influence the overall conclusions of the study:

- Not all airlines publish reports: it is therefore impossible to conclude anything on their risk management practices.
- Not all airlines report all what they do: airlines choose to publish the information that they seem relevant for the prosecution of their objectives; what is included in the annual reports may or may not cover the full process details, risk landscape or mitigation measures put in place. Airlines are entitled to not disclose sensitive information, decisions and processes.
- There is no guarantee that reported practices are accurate and/or effectively implemented: as some airlines did not reply to clarification questions, there is no possibility to verify the full validity and effectiveness of reported statements. One must rely on the goodwill of these airlines, trusting what is reported.
- Looking at the Top 100 airlines does not fully represent the airline community and hence their risk management practices. IATA has over 240 airline members with scheduled passenger and/or cargo operations, large and small. Flightglobal's database of air transport operators lists in 2013 a total of 1879 active companies, and 1935 in 2014. Given the large size and variety of the universe, the above approach was considered valid to gather a high-level picture of what the world's major airlines are doing (or reporting) on risk management topics.
- Such a survey, focused on a few issues under analysis with limited answering options, limits the depth of the analysis. Therefore a more detailed qualitative evaluation complementing the quantitative survey is included in the next section.

Given that there is no other updated source providing the needed information, it was seen as appropriate to continue with this approach. The next sections will outline all quantitative and qualitative results achieved.

5.2.2. Quantitative results: how airlines report risk and risk management practices

From all the 100 airlines included in the survey, 21 did not publish any report or made any specific statements on risk management on their respective websites. These include Qatar Airways, Saudia, Alitalia, Asiana, Air Europa and LOT Polish Airlines, among others.

Of those airlines publishing at least one kind of report, eight do not have any reference to risk or risk management practices: Virgin Atlantic, Air India, UTair Aviation, Eqyptair, AirAsia, Pakistan International, Aerolineas Argentinas and Kingfisher.

One specific airline (S7 Airlines), despite publishing an annual report for 2011, did so in the native language of that airline only (Russian), therefore no conclusions could be taken for this airline due to language limitations.

This reduces the initial group to about 70 airlines for which conclusions can be drawn. Of these, 41 mention risk in their annual report only, 3 comment on it in their corporate governance report only, another 3 in their social responsibility report and the remaining 23 refer to risk and risk management in all of their publicly available reports.

Only two airlines present some kind of risk definition:

- Air France KLM states risks are "events that could potentially affect the Group and prevent it from achieving its objectives" (Air France KLM, 2011, p. 90).
- Air New Zealand states "risk is the effect of uncertainty in the achievement of our key objectives" leaning clearly to the AZ/NZS and ISO 31000 definitions of risk. (Air New Zealand, 2010, p. 1)

Another airline publicly quantified a threshold of materiality. Lufthansa refers to something that can be understood as their attitude towards risk: "Risks count as material if they are capable of causing damage of at least one third of the operating result necessary for maintaining the value of the Company. For 2011 this amount was again determined to be EUR 300m for the Lufthansa Group" (Lufthansa German Airlines, 2012, p. 114). Similar statements from 2003 onwards included lower values; the 2012 annual report keeps the same EUR 300m value with a slightly clarified statement ("In 2012, material risks are defined as those which could result in a loss of at least EUR 300m.")

The remaining airlines do not present a clear definition of risk or their attitude (defined as materiality threshold) towards it.

Only Air New Zealand has a publicly available risk management policy, as a separate document signed by its CEO. This was last updated in 2010 (Air New Zealand, 2010). Singapore Airlines refers to a Risk Management Policy, but does not publish it online.

In terms of the standards used, the following can be concluded from statements made in their 2011 Annual Reports:

- Four airlines specifically refer to ISO 31000:2009 – Singapore Airlines, Thai Airways, South African Airways and Cargolux;
- Two airlines refer to AS/NZS 4360:2004 – Cathay Pacific and Air New Zealand;
- COSO is mentioned by 28 airlines– among them are 21 North and South American airlines (notably United Continental, Delta Airlines, American Airlines, FEDEX, Air Canada, Copa Airlines, TAM Linhas Aéreas and GOL Transportes Aéreos), some European airlines (Lufthansa Group, Air France KLM, the SAS Group, Thomson Airways and TAP Portugal) and two Asian (Malaysia Airlines and Garuda Indonesia).

- Two airlines cite two standards. Qantas uses COSO and ISO 31000: “the Qantas risk management and internal control system aligns to the principles included in the Australian/New Zealand Standard on Risk Management (AS/NZS ISO 31000:2009) and the Committee of Sponsoring Organisations of the Treadway Commission (COSO) framework for evaluating internal controls.” (Qantas, 2011a, p. 25). Finnair says: “the overall system of internal control and risk management in Finnair is based on the commonly accepted COSO ERM framework and ISO 31000:2009 standard for risk management.” (Finnair, 2011, p. 54)
- Two airlines mention the Turnbull report on internal control procedures and requirements for risk management: Aer Lingus and Ryanair, two Irish airlines.
- The remaining 32 airlines do not refer to any international standard, despite presenting a summary of their risk landscapes and how they mitigated these items. Prominent examples include: IAG (British Airways / Iberia), All Nippon Airways, Emirates Group, Japan Airlines and Air China.

The only conclusion to be drawn from here is that North and South American airlines are more prone to use the COSO standard. From all other regions, there are examples that lean more to one or another standard. Yet the majority still does not refer to any standard. So from all top 100 airlines, only 38 refer to a specific standard.

In terms of attention dedicated to presenting risks these airlines are exposed to, only Lufthansa presents a Risk Report, although it is integrated in the Annual Report and Consolidated Management Report (Lufthansa German Airlines, 2012). Fifty airlines present a full chapter, 17 others just a few paragraphs in their respective management reports.

The internal organisation and ownership of risk reflected in the annual reports shows that 37 airlines make references to the integration of the risk management function with the Internal Audit unit. Six airlines refer to the existence of a dedicated risk management department; two have centralised risk management functions and another two decentralise the management of risk to individual business units and departments. Twenty airlines did not specify how their risk management organisation is.

Relevant statements found in the analysis include:

- United Continental, “In 2010 we became the first airline in the industry to apply risk management principles to all procedural changes related to safety.”
- Finnair, “A dedicated risk coordinator position has been established in 2012 to provide policy implementation support for segments and functions, and consolidate and review reporting on risks and risk management activities.”
- Royal Jordanian Airlines, “Risk management is carried out in cooperation with the Board of Directors and the Executive Management. The Board of Directors makes

sure that the Executive Management implements an efficient and effective system for internal control."

By the statements included in their Annual Reports, 53 airlines include risk management in their corporate governance models. The remaining 47 do not specify this clearly.

The airlines also show how their risk management reporting and discussions take place. Major risks are discussed at the Board of Directors, as mentioned by 45 airlines, although some have Risk Management Committees that either report directly to the Board of Directors or to the Internal Audit Committee. Nine refer to the existence of such an Internal Audit Committee. Fifteen airlines do not specify how risk is discussed at an upper management level.

Lufthansa states that their Risk Committee is "made up of the eight directors of Corporate Controlling, Legal Affairs, Corporate Finance, Corporate Accounting, Corporate Audit (permanent member without voting rights), Corporate IT, Controlling Lufthansa Passenger Airlines and Delvag Group. [And that this committee] is responsible for continuously improving the effectiveness and efficiency of the risk management system" (Lufthansa German Airlines, 2012).

Singapore Airlines states: "A set of Risk Management Principles adapted from ISO 31000 provide the underlying basis for the scope and objectives of the risk management effort, complementing the overarching philosophy provided by the Risk Management Policy Statement as follows: "SIA is to be a risk-aware organisation such that the taking of risks necessary for the achievement of its corporate objectives is carried out knowingly, and risks that represent a threat to SIA are managed so as to protect and enhance the value of the organisation in the interests of shareholders and stakeholders of SIA" (Singapore Airlines, 2012, p. 37).

As for types of risks mentioned, the possibilities included:

- The standard set of risks, considered as being fuel price increases and related hedging activities, credit and liquidity issues, foreign currency fluctuations and safety. This simpler approach in detailing the risks they are exposed to is used by 28 airlines. Interestingly the majority of these (21) do not specify the use of any risk management standard.
- A broader list of company specific elements, related to their own environment, providing details on how the company addresses what is unique to its operation. Three airlines fall into this category: Etihad Airways, Royal Jordanian and Monarch.

- Both options above including industry-specific and macro-economic elements, showing the full coverage of all possible risk sources. 39 airlines report more than the standard or company-specific risks; 24 of these lean to COSO's risk management approach, 3 to ISO 31000 and 8 do not specify the risk management standard used in their organisation.

Further interesting conclusions can be drawn when the above statements and results are compared with the financial results achieved by the airlines over a 4-year period. Source for this information is – again – the Airline Business World Airline Rankings for the years 2008-2011 that consolidate operational and net profitability levels of these airlines.

Before discussing these results, it is important to note that regardless of any conclusions to be drawn from this comparison, there is no evidence that financial results achieved are due to the existence of risk management activities. This comparison does not intend to be a scientifically and statistically valid correlation study. Moreover, financial results included are as reported by the Airline Business magazine, which have not been verified or validated. Averages shown include only those airlines that have reported results.

Based on the above, comparisons were made to answer the following two questions:

1. Do airlines that publicly report on risks and risk management practices have better financial performance, than those who do not?
2. For those airlines that make references to one specific standard, does their financial performance stand out from all others?

To answer the first question, the results of Question 8 of the survey were used and put against the average of net and operating margins achieved by the respective airlines in the four years under analysis. The table below summarises these results.

In terms of operating as well as net margins, those 8 airlines that publish reports without any references to risks or risk management achieve an average financial performance that is clearly below that of the remaining 70 airlines that refer to risk and risk management in their annual reports. Interestingly their performance is also below those airlines that do not publish any report. This is true for all four years under analysis.

One could say that the large volume (8 against 70) influences the average achieved, especially when those 8 include large loss-making airlines. Looking deeper into the results, the list includes highly negative operations such as Kingfisher Airlines (in 2011 -20,9% operating margin and -41% net margin, with similar negative results in other years); Aerolineas Argentinas (in 2010 -41,4% operating margin) and Air India (in 2010 -26,2% and

in 2009 -41,2% operating margin). But this list also includes large profit making airlines such as Air Asia (26,8% operating margin in 2011; 27% in 2010; 28,7% in 2009; and 13% net margin in 2011; 27% in 2010; 16% in 2009), UTair and Egyptair with positive, but more modest results. Virgin Atlantic only shows results for 2008, slightly positive for both operating and net margins (1% and 3% respectively).

Table 2: Average financial performance 2009-2011 vs references to risk management

Question 8: Is Risk Management mentioned in any report?	Count of Airline	Average of Operating Marging 2011	Average of Operating Margin 2010	Average of Operating Margin 2009	Average of Operating Margin 2008
No	8	-2,25%	-4,99%	-8,16%	-15,57%
Yes	70	3,61%	6,73%	3,39%	-0,32%
(blank)	22	4,08%	6,30%	-1,42%	-5,49%
Grand Total	**100**	**3,40%**	**5,72%**	**1,91%**	**-2,26%**

Question 8: Is Risk Management mentioned in any report?	Count of Airline	Average of Net Margin 2011	Average of Net Margin 2010	Average of Net Margin 2009	Average of Net Margin 2008
No	8	-12,75%	-9,17%	-12,60%	-19,80%
Yes	70	1,44%	4,50%	1,31%	-4,38%
(blank)	22	-0,75%	4,13%	-3,63%	-5,63%
Grand Total	**100**	**0,43%**	**3,50%**	**-0,32%**	**-5,66%**

Source: (Airline Business, 2012), own comparisons

The same way, the 70 airlines that have risk references in their reports include some loss making companies (although less in number, smaller in losses and with losses in fewer years). Examples are Malaysia Airlines (-16,5% operating margin in 2011) or Japan Airlines (-10,6% in 2009), both with profits in other years. It also includes large profit makers, such as Copa Airlines, Ryanair or Atlas Air with mostly double digit operating profit margins.

Therefore, as answer to question 1 above and taking all disclaimers into account, the tendency would be to say yes, airlines with references to risk management seem to have better average financial performances. This makes sense, given that the goal of risk management is to help organisations have better control and contribute to an operationally and financially sustainable operation.

As for the second question, comparing the use of a specific standard to the actually achieved financial results, no clear trend or relationship can be seen. In some years, airlines using AS/NZS 4360 achieve high operating and net margins (2010 and 2009), in other years it is the group of airlines that reference Turnbull (2011).

The table below summarises the average operating and net margins achieved by these 100 airlines over the 2008-2011 period. No clear conclusion can be drawn.

Table 3: Average financial performance 2009-2011 vs use of a specific standard

Question 11: What standard is mentioned?	Count of Airline	Average of Operating Marging 2011	Average of Operating Margin 2010	Average of Operating Margin 2009	Average of Operating Margin 2008
AS/NZS 4360:2004	2	4,05%	9,70%	5,15%	-0,80%
both	2	1,00%	0,65%	1,40%	8,70%
COSO	28	3,44%	5,99%	4,24%	0,85%
ISO 31000	4	0,30%	10,30%	1,50%	-0,38%
not specified	32	3,72%	7,21%	3,01%	-1,40%
Turnbull	2	9,70%	8,90%	-0,30%	-4,40%
(blank)	30	2,50%	2,54%	-3,40%	-8,67%
Grand Total	**100**	**3,40%**	**5,72%**	**1,91%**	**-2,26%**

Question 11: What standard is mentioned?	Count of Airline	Average of Net Margin 2011	Average of Net Margin 2010	Average of Net Margin 2009	Average of Net Margin 2008
AS/NZS 4360:2004	2	4,00%	9,00%	3,50%	-2,50%
both	2	-1,00%	0,00%	1,00%	6,00%
COSO	28	-0,04%	3,12%	2,74%	-4,41%
ISO 31000	4	-1,33%	5,50%	-2,00%	-1,25%
not specified	32	2,42%	5,40%	0,17%	-5,31%
Turnbull	2	9,50%	7,00%	-0,50%	-7,00%
(blank)	30	-3,75%	0,50%	-7,08%	-11,08%
Grand Total	**100**	**0,43%**	**3,50%**	**-0,32%**	**-5,66%**

Source: (Airline Business, 2012), own comparisons

5.2.3. Qualitative results: examples of risk management models at airlines

The above process involved reading, assessing and classifying the annual reports, corporate governance reports, sustainability reports and other public documents issued by these top 100 airlines on their websites. During this process several qualitative elements could be identified, showing the airlines' approaches in graphical models or other formal statements regarding their risk management practices. This section will therefore complement the more quantitative analysis presented earlier, highlighting some of the most interesting models in an attempt to gather more information on how airlines manage risk.

Anticipating some of the possible conclusions of this section, it can be said that there is no visible commonality among the various approaches presented and described by these airlines in their respective annual reports. Naturally some elements may coincide, such as a matrix-based risk evaluation, but the way these are described and presented is fundamentally different. While Qantas, for example, is quite transparent in reporting all it does on risk management, some other airlines are rather cautious in disclosing their risk assessment process, the risk evaluation matrix or risk tolerance approval levels. Also in terms of organisation the next sections will show a variety of different models: from being split among several business units (Japan Airlines) to being integrated into one corporate and group wide unit reporting directly to the executive board (Lufthansa).

More than presenting similarities, the selected examples will show the differences in organising risk management approaches and units at the various airlines.

5.2.3.1. Qantas Group

From all airlines looked at, or at least from those 70 publishing any kind of management report, the most complete approach on risk management seemed to be from Qantas. Not only do they publish a vast collection of corporate documents, most with references to risk management responsibilities and procedures, but it was also possible to find the Qantas Group Risk Assessment Guide[13] (Qantas, 2012b). The published documents include:

- Qantas Group Annual Report 2011 (Qantas, 2011a), outlining major investment, commercial and distribution issues, as well as operational activities conducted during the year; corporate governance reports, financial results achieved and therein their approach to risk management;
- Qantas Group Audit Committee Charter 2011 (Qantas, 2011b), with roles and responsibilities attributed to the Audit Committee, including the responsibility to assist the board in fulfilling corporate governance guidelines, i.e. risk management;
- Qantas Group Data Book 2011 (Qantas, 2011c), showing a historic 10-year overview of key financial and operating statistics, passenger and market share data, fleet structure, environmental analysis, detailing therein the Qantas Risk Management Culture;
- Qantas Group Constitution (Qantas, 2010), with no direct reference to risk or governance issues, but establishing the basic rules that guide the entire operation;
- Qantas Group Business Practices Document (Qantas, 2012a), describing how they want to do business, including a chapter on how to manage risks; and finally
- Qantas Group Risk Assessment Guide (Qantas, 2012b), acting as a quick reference guide for risk management with hands on practical descriptions, explanation of threshold levels, responsibilities and risk tolerance approvals.

There were also references to a Qantas Risk Management Policy, which could not be found.

The Annual Report refers to the Boards' risk management functions (Qantas, 2011a, p. 25):

- "The Board is responsible for reviewing and overseeing the risk management strategy for the Group and for ensuring the Group has an appropriate corporate governance structure. Within that overall strategy, Management has designed and implemented a risk management and internal control system to manage Qantas' material business risks."
- "To manage these and other risks, the Board is responsible for reviewing and approving the Qantas Group Risk Management Framework. The Framework is underpinned by three interrelated elements: governance, risk management and assurance."

[13] This document – also called *QRAG* – states, interestingly, that it is for "internal use only" and "not to be distributed externally". Nevertheless it was easily found online, browsing for "Qantas Group Risk Assessment Guide".

- "The Board also reviews and approves the Qantas Group Risk Management Policy, which sets out the minimum requirements, and roles and responsibilities for managing risk across the Qantas Group."
- "The Qantas Management System (QMS), which has been implemented across the Group, provides a common standard for identifying, assessing and managing material business risks across the Group."
- "Material risks and the effectiveness of risk management plans are escalated to Executive Management, Relevant Board Committees and/or the Board as appropriate and are reported on as part of the quarterly risk reporting process. During the quarterly risk reporting process, each Qantas Group business unit prepares and submits a detailed risk register outlining the key risks to achieving their objectives and mitigating actions."

Graphically, the interrelation between these documents is depicted in the QRAG.

Figure 64: Qantas Group Risk Assessment

Source: (Qantas, 2012b, p. 1)

The Qantas Data Book outlines the elements of their Risk Management Culture, including:

- Leadership and commitment, and the support and endorsement given by the board and top management to implement the risk management process;
- Risk management resources, notably risk champions throughout the company, involving all departments in this continuous effort;
- Integration into decision making processes, delivering input for strategy development, project and contract management;
- Building consistent risk capabilities, via risk training and awareness creation;
- Independent reviews of the whole framework to keep it updated and correct gaps. (Qantas, 2011c, p. 83)

From these documents, it is also possible to understand that Qantas uses a 6-by-6 risk assessment matrix for consequence (from 'negligible' to 'catastrophic') and likelihood ratings (from 'almost certain' to 'very rare'), each with quantitative or qualitative descriptions of each category. The consequence ratings are assessed in terms of financial impact (e.g. 'catastrophic' relate to events with financial impact – in terms of profit, cost or revenues – of over AUD $200 million). The likelihood is assessed in terms of probability (e.g. the 'almost certain' classification is for events with more than 95% probability of occurring). The resulting risk matrix is depicted below.

Figure 65: Qantas Risk Matrix

	Consequence					
Likelihood	**1. Negligible**	**2. Insignificant**	**3. Minor**	**4. Moderate**	**5. Major**	**6. Catastrophic**
A. Almost certain	L	M	H	E	E	E
B. Likely	L	M	H	H	E	E
C. Possible	VL	L	M	H	H	E
D. Unlikely	VL	L	L	M	H	H
E. Rare	VL	VL	L	L	M	H
F. Very rare	VL	VL	VL	L	M	M

Risk level	VL	Very low	L	Low	M	Medium	H	High	E	Extreme

Source: (Qantas, 2012b, p. 4)

There is a tolerance approval process, that requires immediate notification to or formal approval from the functional superior. The QRAG states that "'extreme' and 'high' risks are generally not tolerable" and that "Other risk levels, may be tolerable at Management's discretion, although there is a lower tolerance for Safety and Compliance risks."

Figure 66: Qantas Risk Tolerance Approval

Current Risk Level	Very low	Low	Medium	High	Extreme
Immediate Notification (or equivalent business unit level of authority)	Supervisor	Manager and Supervisor	Heads of and Managers	Group Executives, Executive Managers	Chief Executive Officer, Group Executives
Tolerance Approval (or equivalent business unit level of authority)					

Source: (Qantas, 2012b, p. 4)

Associated to each risk and risk level is an action development and implementation timeframe that can require 'immediate action' for extreme risks or 'maintain focus on existing controls' for risks considered 'very low'.

The QRAG also presents a risk register template where each risk is to be identified, described, ownership attributed, its causes listed, expectable consequences, controls in place, risk ratings (before and after control implementation), actions and due dates.

5.2.3.2. Air New Zealand

While not being as detailed in their reporting, Air New Zealand deserves a special reference as it is the only airline that publishes a Risk Management Policy as a separate document, duly signed by the Chief Executive Officer of the airline.

This 2-page document, last updated on January 26th 2010 (Air New Zealand, 2010), aims at:

- Presenting the airlines' risk policy statement;
- Listing the objectives of such a policy;
- Defining the airlines' understanding of risk and risk management;
- Deciding on risk reporting guidelines, responsibilities; and
- Identifying the contact person for risk management-related matters.

This document is published in the corporate section of the Air New Zealand website, under Corporate Governance and Social Responsibility Policies, such as the Environmental Policy, Group Compliance Policy, Shareholder Communications Policy and Audit Independence Policy.

Air New Zealands' Annual Report focuses mostly on Financial Risk Management, covering the standard aspects of currency risk, equity price risk, fuel price risk and interest rate risks. Other risks are not clearly mentioned in this document. Nevertheless, it is interesting to see that in 2009 in an interview given to the *Airlines International* magazine, the CEO of Air New Zealand stated, regarding risks faced by the airline, that "we can talk about the economic crisis and other industry issues such the price of oil, the environment and so forth, but the biggest challenge for us—the biggest impact on our business—is the delay of the Boeing 787" (IATA, 2009).

Later in time, in the Air New Zealand Interim Shareholder Review 2012, the organisation states "Whilst we are disappointed with the delay in arrival of the B787-9's we have now reached an agreement with Boeing regarding new terms and delivery dates" (Air New Zealand, 2012, p. 4). Not only did it take time to overcome the aforementioned risk, but even with mitigation measures in place the airline is still not operating as it wanted to (with the selected aircraft). This issue affected many airlines, Boeing and Airbus customers, and is a recurrent event with all new-design aircraft being introduced.

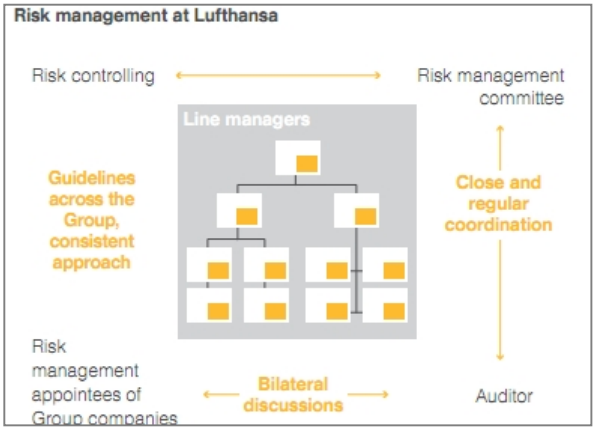
The airline also publishes a Constitution, which is similar in purpose and content to Qantas'.

5.2.3.3. Lufthansa Group

Lufthansa's annual reporting practices are marked by a strong consistency showing a visible evolution of their risk management organisation. Since 2003 (last year available in the online archive) a dedicated chapter dubbed 'Risk Report' (or later 'Risk and Opportunity Report') has always been included in the Annual Report. Each includes a definition and quantification of the yearly risk appetite level. "Major risks are defined as dangers which per se might cause damage equal to at least one third of the result necessary to maintain the Company's inherent value." (Lufthansa German Airlines, 2004, p. 100). This value was first quantified in 2007 at EUR260m, and then evolved over the years to the current level of EUR300m as shown in the 2012 annual report.

A graphical depiction of the risk organisation was also first presented in 2007, stating "the deliberate management of risks and rewards is an integral component of corporate leadership and decision making. There is, therefore, no independent organisational structure for risk management" (Lufthansa German Airlines, 2008, p. 101). This indicates that Lufthansa used, for all but financial risks (the exception is made later in the report), a decentralised approach with no central entity managing the whole risk identification and assessment process.

Figure 67: Lufthansa Risk Management Organisation 2007

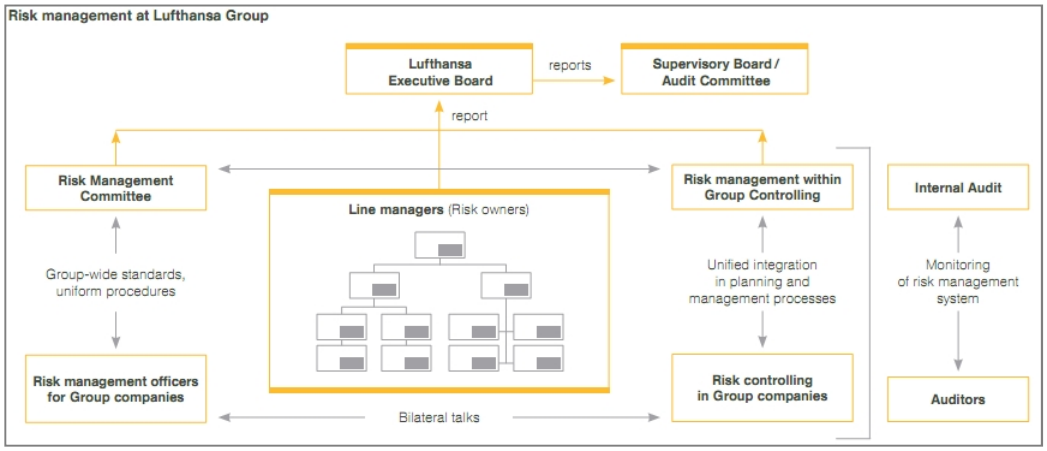


Source: (Lufthansa German Airlines, 2008, p. 101)

A similar structure was kept until 2012, when a new organisation was introduced, showing a central management unit: "As part of a reorganisation of the methods and IT used by the Lufthansa Group risk management in 2012, a system was installed that supports a uniform Group standard for comparing risks and provides a standardised, up-to-date reporting format. It incorporates risk management even more thoroughly in all operating segments,

which makes the risks and associated responsibilities even more transparent. A new, independent risk management unit within Group Controlling is responsible for implementing Group wide standards and for coordinating and continuously improving the risk management process" (Lufthansa German Airlines , 2013). The graphical depiction of that organisation was therefore updated to reflect this change.

Figure 68: Lufthansa Risk Management Organisation 2012



Source: (Lufthansa German Airlines , 2013, p. 105)

It is possible to see that the individual business units and subsidiaries are still responsible for risk management within their organisations, but have to follow the standards, planning and management processes established by group functions. The existence, function and composition of the Risk Management Committee have already been detailed in the previous section. Internal Audit is separate and monitors the whole risk system. All entities report to the Executive Board, that by itself reports to the Supervisory Board.

Earlier in this thesis comments have been made on how Lufthansa considers risk management as one of the three pillars of corporate governance (see Figure 3 – Lufthansa Corporate Governance Model), displayed on Lufthansa's website.

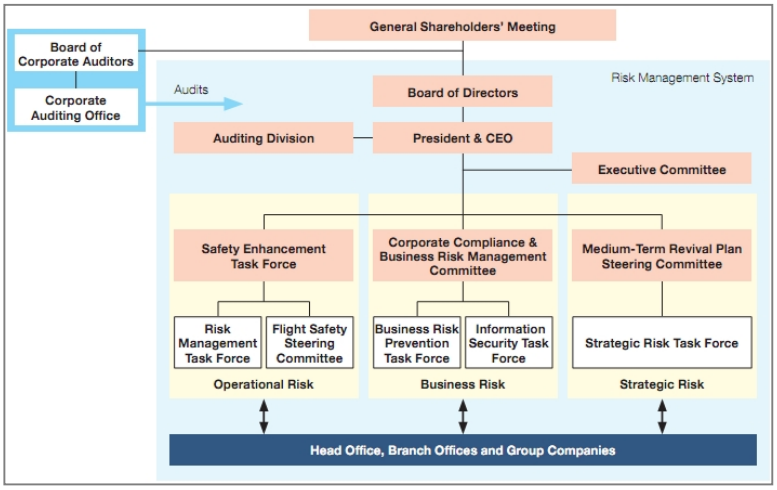
5.2.3.4. Japan Airlines

Despite being in the middle of a corporate restructuring process that saved the airline from bankruptcy, and not publishing any Annual Report since 2009, this case still shows some interesting findings. The 2009 Annual Report includes a depiction of the Group Internal Control Systems with a description of units responsible for the various types of risk. These risks include operational risks related to the air transport business, handled by the Safety Enhancement Task Force; business risks arising from other businesses than air transport,

handled by the Corporate Compliance & Business Risk Management Committee; and strategic risks that can have an adverse impact on the earnings structure, overseen by the Medium-Term Revival Plan Steering Committee (Japan Airlines, 2010, p. 23).

It is possible to see that all internal entities are involved in the risk management system, from Board of Directors to Branch Offices, and that each risk type is handled by a different unit that report directly to the President & CEO of the airline.

Figure 69: Japan Airlines Group Internal Control Systems 2009



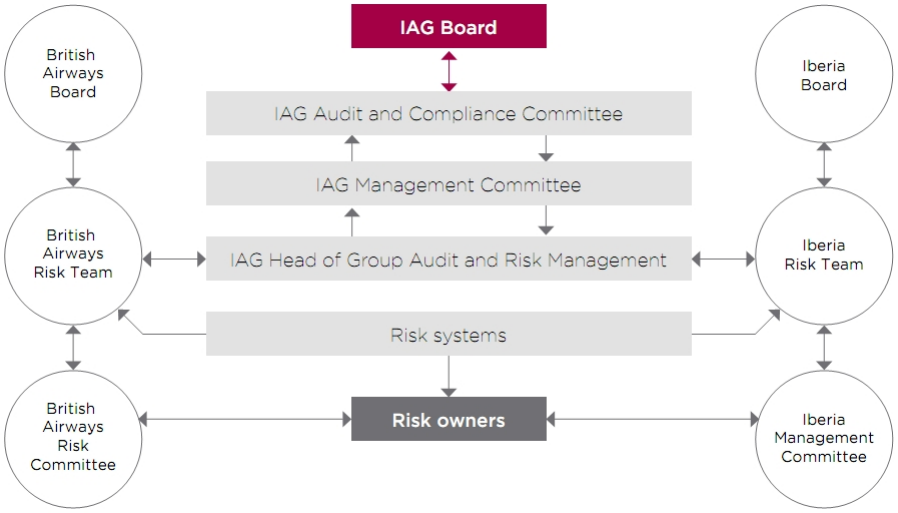
Source: (Japan Airlines, 2010, p. 23)

5.2.3.5. IAG Group – British Airways / Iberia

This case is interesting as it reflects how risk is managed in a merged entity. While it is stated that "the core methodologies within British Airways and Iberia were very similar prior to the merger" these "have been harmonised allowing consolidation of the Group's risk position" (IAG Group, 2012, p. 75). The report refers to the parallel processes running at British Airways and Iberia, the former including quarterly reviews by the Risk Committee (composed of the "British Airways Leadership Team, the Head of Corporate Risk and key senior executives") and the latter having half-yearly reviews conducted by the Iberia Board.

From a content perspective, "the IAG Board discussed risk at a number of meetings including discussions around the Business Plan, major projects and the bmi acquisition. It also discussed the results of the audit and Compliance Committee full review of the group risk map" (IAG Group, 2012, p. 75).

Figure 70: IAG Risk Management model 2011

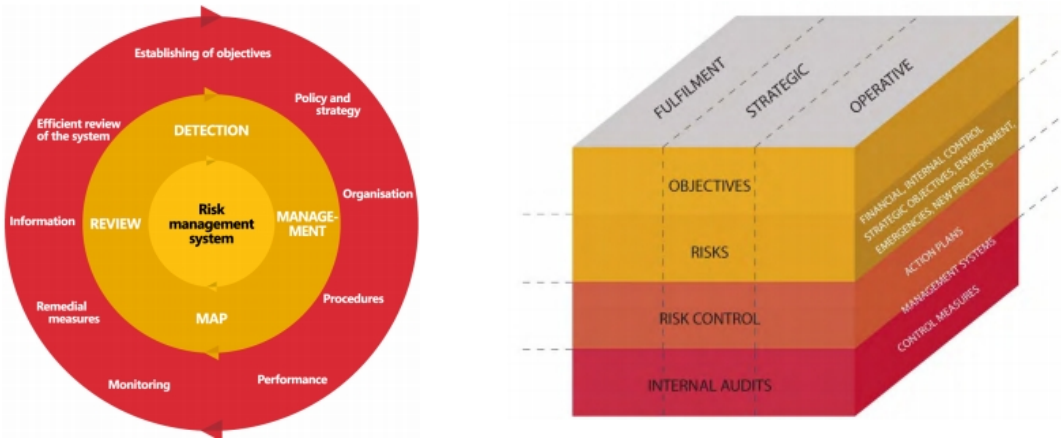


Source: (IAG Group, 2012, p. 75)

In Iberia's last Annual Corporate Governance Report as separate company, for 2009, they published the fundamentals of their risk management system. While the overall framework is adapted from the ISO 31000 standard, there are also some elements of the COSO model. Therein Iberia states: "as a result of its implementation, Iberia not only has its risk exposure under control, but moreover it now also has a systematic risk management, with the following features:

- Each risk has a proprietor, the person ultimately responsible for its management.
- The Risk Map is reviewed every six months at the top executive level, pinpointing any new risks.
- There are defined procedures of approval, management and information.
- Active participation of all those responsible for the System" (Iberia, 2010, p. 188).

Figure 71: Iberia Risk Management System 2009



Source: (Iberia, 2010, p. 188)

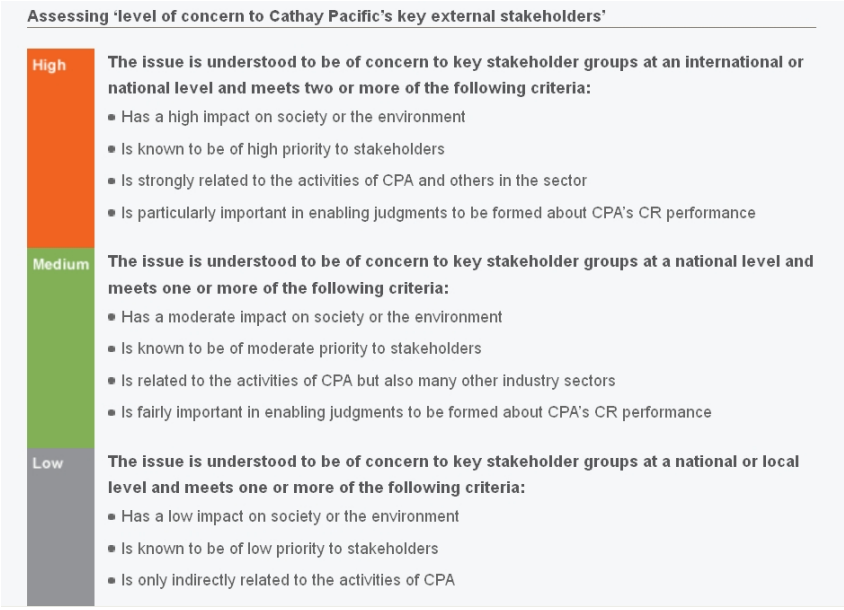
5.2.3.6. Cathay Pacific

This Hong-Kong based airline is very embracing in the way it manages risk, or at least in the way it reports its risk management activities in the Corporate Governance report: not only does it perform company internal risk management, which is integrated into the overall Swire Group risk management process[14], but it also involves stakeholders in the process in a way to get outside contributions on potential issues affecting the airline. All contributions are consolidated into a materiality matrix on sustainability. "An issue is 'material' when it substantially affects our long term commercial and operational viability. This matrix combines the Swire Group approach on identifying the risk concerns of our stakeholders and our own materiality scoring methodology" (Cathay Pacific, 2012, p. 20). The criteria for assessing materiality are shown in the figure below.

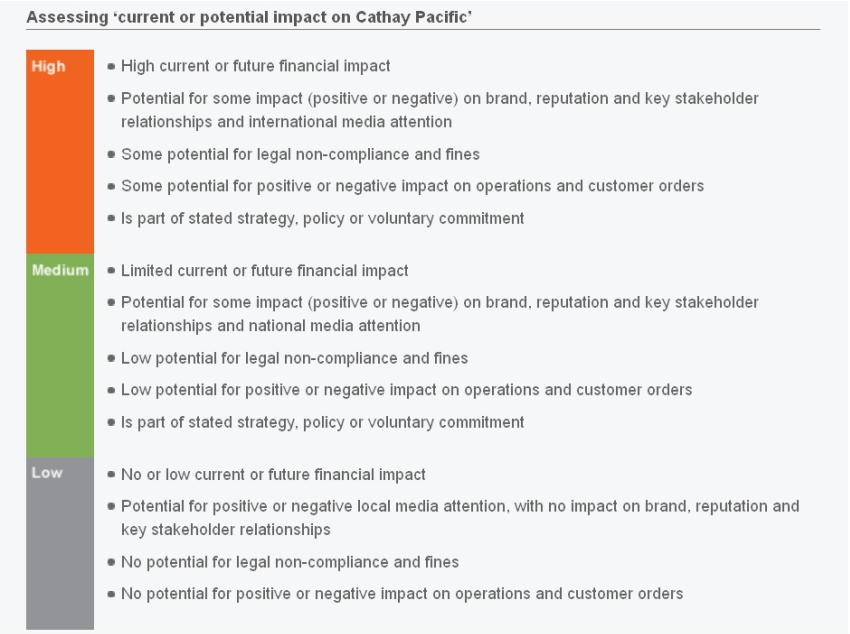
The outcome is the stakeholder issue matrix, crossing an importance rating with multiple stakeholders against the potential impact on Cathay Pacific in two high-low axis following the criteria listed below.

This approach shows how AS/NZS 4360 and ISO 31000 (in the meanwhile adopted by the airline) can be adjusted to the airlines' needs. It goes further by not only involving internal elements, but also external stakeholders in the companies' risk management effort.

Figure 72: Cathay Pacific Criteria for Assessing Materiality 2011



[14] Cathay Pacific airlines is owned in 43% by the Swire Group (Source: FlightGlobal.com).



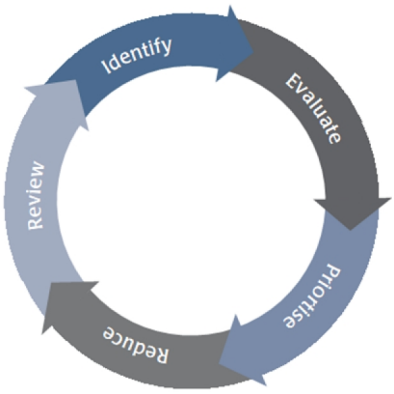
Source: (Cathay Pacific, 2012, p. 20)

5.2.3.7. Singapore Airlines

Singapore Airlines builds its governance and reporting structure around several Risk Management Committees (one per subsidiary), a Central Group Risk Management Committee to whom they report, a Board Safety and Risk Committee that oversees the previous ones and ultimately reports to the Board of Directors. Moreover, "a dedicated Risk Management Department provides support to the Risk Committees and to business units, ensuring that risks are surfaced by business units from the bottom up to complement the top-down perspectives provided by top management and the Risk Committees" (Singapore Airlines, 2012, p. 36). The Risk Committees have quarterly risk review activities.

The governing philosophy is based on ISO 31000, upon which a simplified circular 5-step Risk Management process has been adopted "to allow easier communication, understanding and application by all levels of staff". These steps comprise: risk identification, risk evaluation, risk prioritisation, risk treatment and review.

Figure 73: Singapore Airlines simplified 5-step Risk Management Process 2011



Source: (Singapore Airlines, 2012, p. 37)

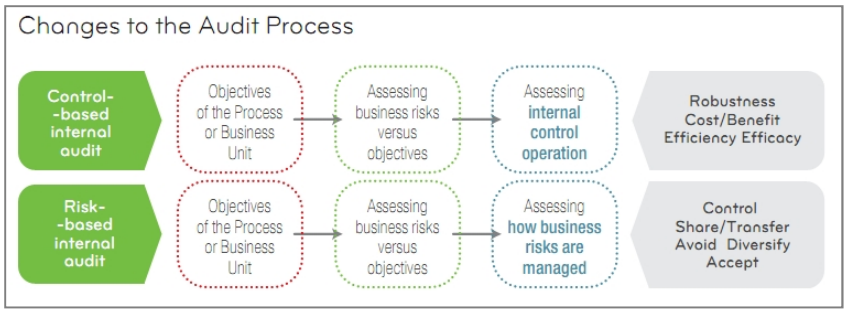
Singapore Airlines states that this is an "embedded activity" where all business units are called in to participate in the Group-wide risk review occurring twice each year.

"Within this process, multi-pronged Risk Reduction strategies such as Risk Prevention, Risk Mitigation and Risk Transfer are employed to address the risks. Wherever possible, preventive measures are adopted and complemented with Crisis Management, Business Continuity and Disaster Recovery plans that are coordinated and integrated into a seamless risk response effort. Risk policies, guidelines and tolerance limits are incorporated into the process to ensure adequacy and effectiveness of risk responses" (Singapore Airlines, 2012, p. 37).

5.2.3.8. TAP Portugal

This airline presents a risk management framework that leans towards the COSO guidelines, but focusing on two distinct areas: one operational addressing business specific aspects, therefore controlled by the business unit leaders, and one transversal controlled by the Internal Audit function of the airline. This way, TAP evolved from an Internal Audit focused on control to a risk-focused Audit. While the starting point always revolves around assessing the business risks versus company objectives, the main difference resides in the content: the control-based audit aims at assessing the internal control of the operation and the second looks at assessing how business risks are managed[15].

Figure 74: TAP Portugal Risk-focused audit process 2011



Source: (TAP Portugal, 2012, p. 19)

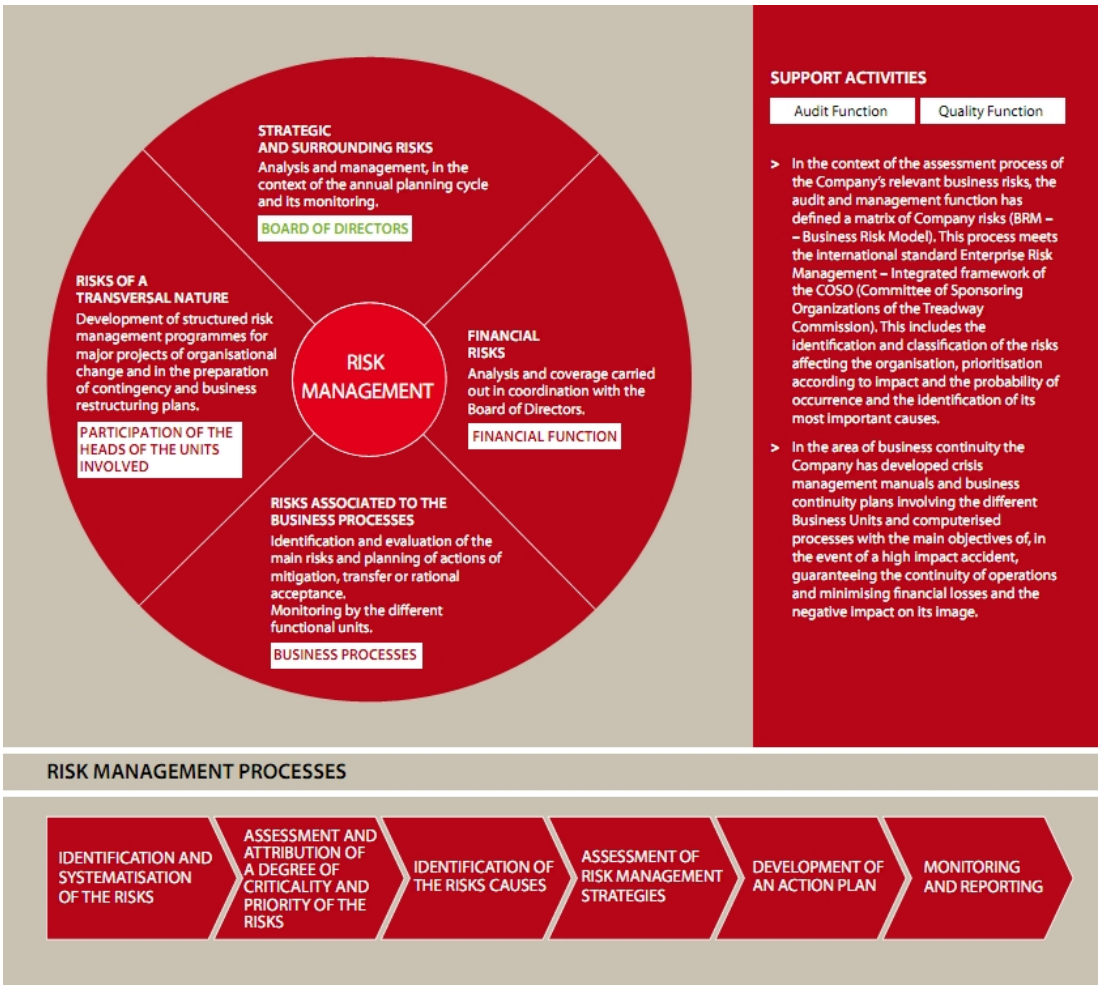
In its 2009 Corporate Governance and Sustainability Report, the airline published a more detailed description of the entire approach, showing the various stages of the risk management process and allocated responsibilities. Therein a 6-staged process is visible, comprising: identification and systematization of risks, risk assessment, root cause analysis, assessment of risk management strategies, action plan development and a final monitoring and review step.

It is also shown that each risk type was handled by different elements within the organisation:

- Strategic Risks were handled by the Board of Directors;
- Financial Risks by the Finance Department;
- Transversal risks were handled by the involved respective business units; and
- Business process risks were taken care of by the business process owners.

[15] TAP Portugal did not reply to a contact request to clarify their risk management approach.

Figure 75: TAP Portugal Risk Management process 2009



Source: (TAP Portugal, 2010)

5.2.3.9. TUI Travel

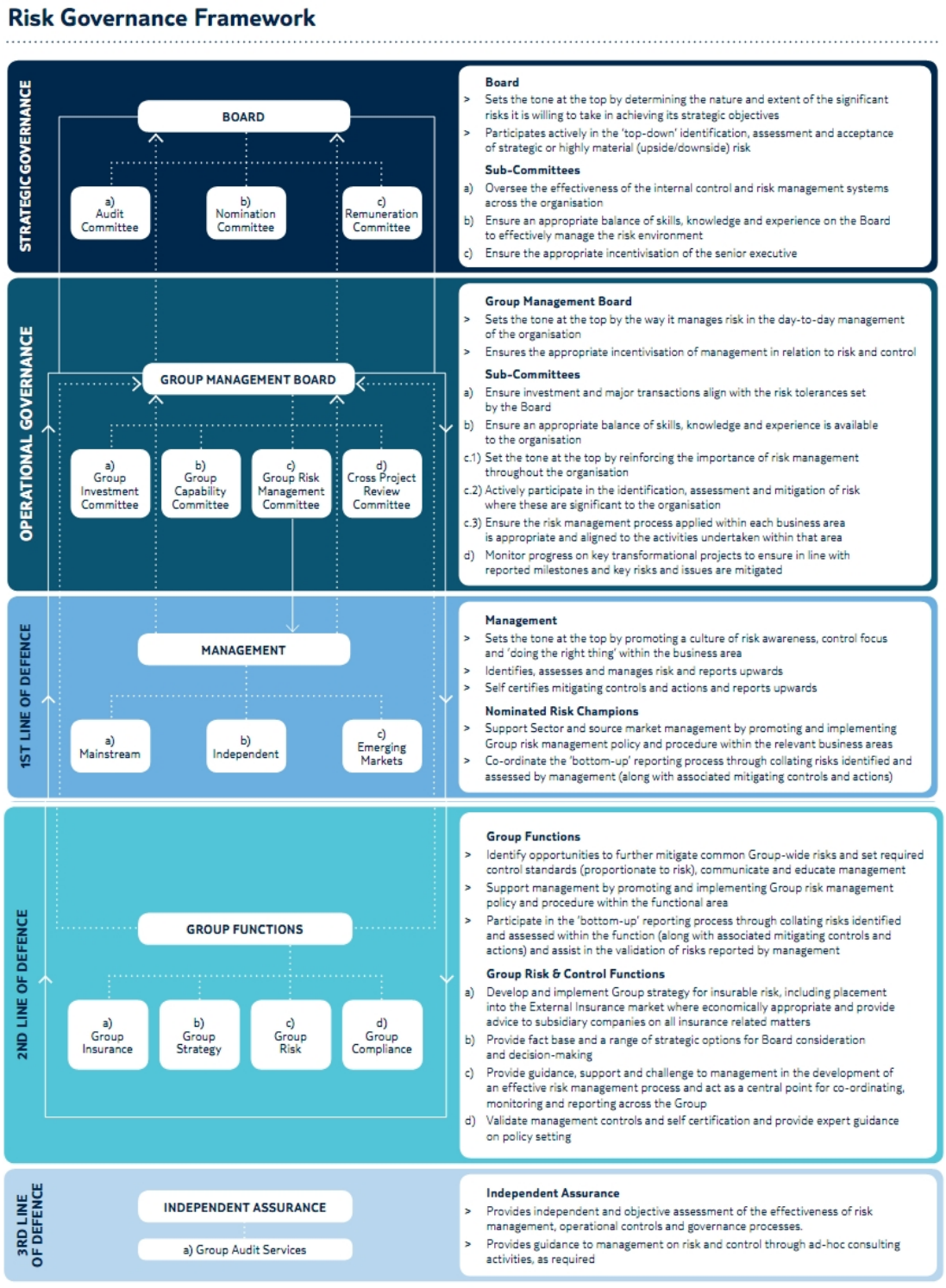
What makes the TUI Travel reports so interesting is their presentation of a 'risk aide memoire', their naming of the risk landscape they are exposed to, and especially their risk governance framework, which is quite detailed in showing involved entities and their three lines of defence model (the latter in the 2012 edition of the Annual Report).

"Whilst ultimate responsibility for risk management rests with the Board, effective day-to-day management of risk rests within the business. Management is responsible for setting the right tone at the top and establishing a culture where employees are expected to be risk aware, control minded and to 'do the right thing'" (TUI Travel, 2013, p. 20).

This report details the risks *of* the companies' strategy and the risks *to* their strategy, while elaborating on the process, responsibilities, etc. It is probably the only airline that considers 'risk velocity' as "the speed at which risks can materialise into issues", instead of the more

traditional likelihood measured as probability of occurrence, when it comes to assessing and evaluating each risk. The other element is still the traditional impact on the organisation.

Figure 76: TUI Travel Risk Governance Framework 2012



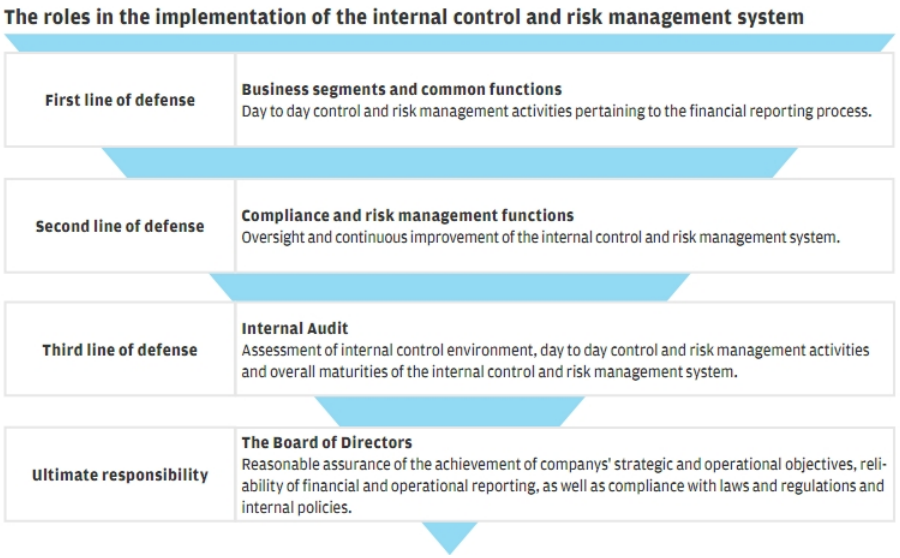
Source: (TUI Travel, 2013, p. 21)

The aforementioned three lines of defence include management, group functions and independent assurance. All these are integrated into the operational governance of the company and report to the Board, as strategic governance body. A similar three-line of defence model is also used by Finnair and Garuda Indonesia.

5.2.3.10. Finnair

Being different in graphical depiction, Finnair's three line of defence model relies on common business segment management, compliance and risk management functions and internal audit, before issues are taken to the Board of Directors as ultimate responsible.

Figure 77: Finnair three lines of defence 2012



Source: (Finnair, 2013, p. 54)

"The objective of internal control and risk management system in Finnair is to safeguard the company's assets and provide the Board and the Executive Management with a reasonable assurance of the achievement of company's strategic and operational objectives, reliability of financial and operational reporting, as well as compliance with laws and regulations and internal policies" (Finnair, 2013, p. 54).

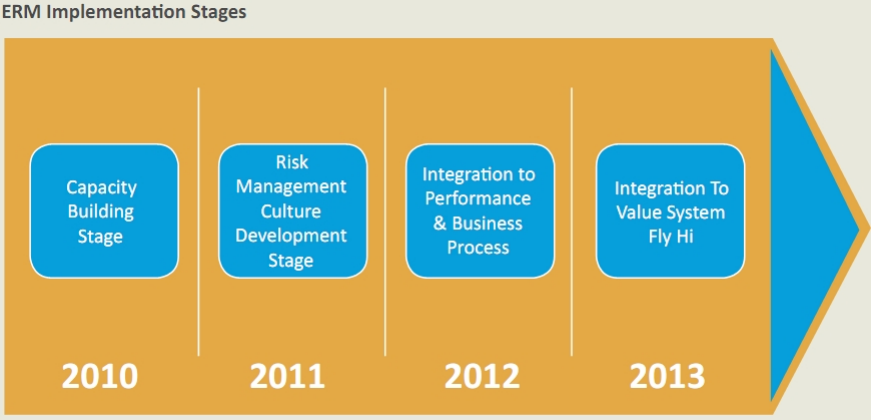
In terms of organisation, "a dedicated risk coordinator position has been established in 2012 to provide policy implementation support for segments and functions, and consolidate and review reporting on risks and risk management activities", indicating that the airline had previously a more informal or decentralised risk management function (Finnair, 2013, p. 55). Elsewhere in their corporate reports a stakeholder analysis and their contribution to risk management is presented.

5.2.3.11. Garuda Indonesia

Garuda Indonesia started implementing the COSO Risk Management Framework in 2010, planning a 4-year horizon to achieve full maturity. The first year was dedicated to a "capacity building stage", creating a risk awareness culture, policy formulation, competency development and structure creating. The second year, called "Risk Management Culture Development Stage", aimed at enhancing personnel capabilities to identify and assess risks. This step also foresaw the creation of a risk management manual.

Stage 3, launched in 2012, aimed at integrating strategic planning and business processes; Stage 4 planned for the internalisation of risk management into the newly developed organisational values.

Figure 78: Garuda Indonesia ERM Implementation Stages 2011



Source: (Garuda Indonesia, 2012, p. 270)

It is certainly still early to say if any results have been achieved or if the process is running smoothly[16]. In any case this shows that implementing a risk management framework takes time, especially because changing corporate culture by creating awareness is not easy.

Garuda also presents a 4-layered defence system in order to guarantee proper implementation and process effectiveness. The first layer is controlled by risk owners, the second by the central Risk Management unit; the third is covered by Internal Audit and the last by Board of Commissioners. Each of these layers takes over responsibilities for implementation, communication, review, monitoring and controlling the whole process.

[16] Garuda Indonesia did not reply to a contact request to clarify the implementation progress and success of their risk management approach.

5.3. Summary of interviews conducted

As initially described, one key aspect of this thesis was to have as much direct input and involvement from the industry as possible. To achieve that, a panel of airline executives and risk managers, practitioners, researchers and lecturers were identified for interview and questionnaire purposes. For this work package[17] alone over 40 organisations and experts were contacted to provide contributions via face-to-face meetings, telephone interviews or structured written questionnaires. Even though some of these companies and individuals never replied to these invitations, a total of 30 individuals from 26 different organisations answered positively. The figure below lists all contributors to this step.

Figure 79: Interview and questionnaire partners

Interviews		
Type A Risk Professionals	**Type B** Airline Representatives	**Type C** Other industries
▪ **Mr. Kevin Knight** Risk specialist and lead author AS/NZS4360 and ISO31000 ▪ **Mrs. Sandra Lonsbury** Senior Vice President Aviation Risk Advisory Solutions, Marsh ▪ **Mr. Mark Hue Williams** Head of Strategic Accounts Aeropspace, and **Mr. Steve Doyle** Sales & Development Aerospace Willis ▪ **Mr. Keith Baxter** Risk consultant and author ▪ **Mr. José Castellanos** QSL Consultores – IATA strategic partner Risk Management ▪ **Ms. Heather Fitzgerald** Risk consultant and trainer, Aerosafe Risk Management ▪ **Mrs. Ayse Kucuk Yilmaz** Risk lecturer and researcher, Anadolu University - Turkey ▪ **Mr. António Fernandes** Secretary General APOGERIS, Portuguese Association of Risk Management and Insurance ▪ **Mrs. Isabel Guimarães** Manager Risk Advisory Services, KPMG Portugal	▪ **Mr. Luiz Lapa** CEO Portugália Airlines ▪ **Mr. António Menezes** CEO SATA Group ▪ **Mr. Yevgen Treskunov** EVP Strategy & Development, Ukraine International Airlines ▪ **Mrs. Ntshabiseng Ntshalintshali** Chief Risk & Compliance Officer South African Airways ▪ **Mr. Steve Tunstall** Former Head of Corporate Risk Management, Cathay Pacific ▪ **Mr. Shane Haberle** Director Risk Management / Chief Internal Auditor Air New Zealand ▪ ***undisclosed*** Director Risk Management, Large German aviation group ▪ **Mr. Olafur Briem** Director Risk Management Icelandair Group ▪ **Mr. John Dombrick** former Head of Entreprise Risk and Business Continuity British Airways ▪ **Mr. Alan Buchanan** Chief of Staff /Company Secretary, British Airways ▪ **Mr. Edmond Rose,** Commercial Director Virgin Atlantic Airways ▪ **Ms. Elaine Liew** Risk practitioner and trainer, former Manager Strategic Risk Management Unit Malaysia Airlines ▪ **Mrs. Carole Gates** Director Risk Management and Insurance, IATA International Air Transport Association	▪ **Mr. Paul Merrick** Head of Quality and Risk, and **Mr. Adrian Sayce** Head of Safety Investigation and Data Department UK Civil Aviation Authority ▪ **Mr. Martin Mueller** Director Alliance Development, **Mr. Santiago Nauffal** Manager Network Planning , **Mr. Mark Rodrigues** Regional Director EMEA Star Alliance ▪ **Mr. Henrique Oliveira** Group Risk Management EDP Energias de Portugal ▪ **Mrs. Ana Figueiredo** Director Risk Management / Chief Internal Auditor Portugal Telecom

[17] See Figure 39: Global project approach and Section 3.2 Work package description

The large majority of these interview and meeting partners are from the airline or the wider aviation industry. Some are from other businesses. The contributions from the latter shall also be used in the next chapter, on lessons learned from other industries.

Some of these individuals preferred to remain anonymous, not disclosing name or organisational affiliation; others specifically asked not be quoted in the text. To respect all these requests, the next sections will summarise contributions in a neutralised manner.

Every individual had different time availabilities, willingness to share information in written and/or oral format, and different styles – some answering very concisely and directly to all questions, others being more cautious in replies given. Some see the topic as commercially sensitive, thus chose not to answer some of the questions asked.

In any case, all face-to-face or telephone interviews, as well as written questionnaires, tried to gather input on current risk management processes, decisions and issues within the company he or she is or was working for, or generic information they might have from other companies, risk discussion platforms or industries.

To better discuss their contributions, this section has been structured around four topics: the context of risk management in the respective organisation, the process that has been implemented and is being followed, organisational issues in terms of risk ownership, roles and responsibilities, and other relevant topics addressed during the talks.

5.3.1. Context

One key conclusion from all interviews conducted is that risk management is, still today, not a wide-spread activity, accepted or even understood by the large majority of airlines. One interviewee stated that most airlines don't have resources or knowledge to do an enterprise-wide risk management effort, although managing operations' risk is normally not a problem. For another interviewee it seems clear that most airlines focus on flight safety and maintenance, because these areas are widely regulated by national and international regulations.

Risk management is also not an area where airlines cooperate with each other, neither at bilateral level nor at multilateral level, using for example industry discussion groups or airline alliance partners. Several airline representatives did not see the value of discussing risks or risk management approaches at such forums, as circumstances, attitudes and

perceptions were always different. In some cases risk and risk management are understood as commercially sensitive matters, therefore discussing them would not only disclose strategic information, but also open ground for anti-trust and competitive lawsuits as these activities might be seen as critical.

One airline representative stated that in the early 2000's, when modern enterprise risk management was not yet developed, the concept of risk was synonymous to insurance. No surprise that many airlines had (and still have) unified departments handling risk and insurance issues – even IATA still consolidates both topics in one management unit. The trigger for this airline to introduce risk management was the severe financial impact of a non-safety related event.

One airline stated that financial risk management was developed after different major events caused changes of the airline performance, such as the fuel price jump in 2004-2008, the global economic and financial crisis in 2009-2011 and the market liberalization in 2006-2012. This airlines' representative stated that the introduction of this financial risk management function allowed the airline to turn from losses in 2010-2011 (after a profitable decade before) to breakeven in 2012. The main results were visible within just 6-12 months. Other risks such as safety and operations related items were handled by the safety risk management function and procurement risks were managed by the audit team. This airline does not have a centralized risk management unit and seems not to manage non-financial, non-safety, non-procurement risks – allocating the management of these, if and when they occur, to one of the established functions in the airline.

At another airline, what triggered the introduction of risk management was the increased risk awareness and new trends in the subjects of internal auditing and risk management. Financial risk management was well established, but centralized systematic enterprise risk management was non-existent although it probably was exercised on an ad-hoc basis.

Yet another airline representative stated that risk management had been gaining importance within the national corporate governance guidelines forcing companies to have visible and dedicated risk management activities. While for many years this airline had a centralized Financial Risk Management department covering financial risks, remaining risks were left to be managed by each business unit and/or departments. Given the change in the guidelines, the board of the airline decided to introduce a centralised unit with the mandate to manage the overall risk management process at the company and group levels,

in order to achieve and fulfil all regulatory requirements. Despite this being quite late in time, this airlines' representative stressed that "one should not say that [we] have not been managing risks or that this new unit comes late. Over the years the process has been maturing, translating itself into a dedicated risk management unit now".

One pioneering airline started quite early with a dedicated risk management function, setting up their own approach and process. While doing this, they produced a benchmarking analysis comparing themselves against other airlines and companies from other industries. While it was clear that the other industry peers were still behind them, the airline understood that lots could be learned from other businesses.

5.3.2. Process

The interviews showed various, sometimes completely opposing, perspectives on risk management. While the definition of risk is mostly common – the impact on objectives; anything that stops the achievement of business plan goals; or even a more simpler version 'anything that worries you' – there are fundamental differences when it comes to the process and approach to managing risk.

One consultant stated that the problem is not the method chosen: it's about management skills. Top management of airline companies are mostly pilots or engineers, not mathematicians. Therefore they would not be able to do or understand the value of a Monte Carlo analysis. The consultant stressed: "we need to talk the same language. Sophisticated methods are a waste of time if management doesn't understand them".

The risk manager of one airline is also very blunt on this: "risk and risk management requires a lot of culture change within the organisation". He stated that it takes time for the organisation to understand risk, and quantified this in roughly 3-5 years. Process-wise it should be as simple as possible, exactly because there are different skill levels involved, the process should not be a hurdle.

There is no clear answer to the question on how the process helps addressing key risks.

Unlike the suggestions above, one airline introduced a more sophisticated method to identify, evaluate and manage risk. This airlines' risk manager states: "We have still a long way to go. But the intentions were to increase risk awareness and somehow put a monetary value to enterprise risk. Some sense of risk culture is emerging and the data is

being collected on a regular basis which is then fed into Monte Carlo simulations for the projected 12 month cash flow for stress testing".

Another, smaller, airline is managing risks on a project basis only (e.g. a new route, a new lounge), whereas individual areas are encouraged to manage their own risks. As the financial area is very exposed, there is a more formal and centralised risk management effort. Key for the success of this model is the small size of the management team: communication is much more informal, therefore decisions are taken much quicker.

At the other end, a much larger airline separates its approach for event-risks and qualitative risks. "For event risks [this airline] uses a traditional risk map with likelihood and probability in a two-dimensional chart. Qualitative risks that cannot be quantified or evaluated or risks that have overwhelming impacts beyond the respective ownership area are looked at using additional attributes. When it doesn't make sense to evaluate items quantitatively, such as those with impact on the extended future, [the airline] remains with qualitative statements."

There is also no clear answer to the question on how a method can best address the airlines' inherent risks within a very specific corporate culture, surrounding environment and management skills and capabilities. As seen above, every airline tends to have a different approach, even when the overall guideline is based on an international risk management standard.

One consultant suggests that an organisation needs to be able to answer five key questions before launching a risk management exercise – and in order to launch it successfully:

1. "What are your processes?
2. What are your inputs?
3. Who are your suppliers?
4. Who are your customers?
5. What are your controls?"

If these are clearly known, then it will be much easier to design a proper approach, define roles and responsibilities and allocate tasks.

One airline has given a clear mandate to their risk management unit: "create added value for decision making processes, while creating a more structured and standardized approach to all risk management activities." This unit has therefore the functions and power to:

- “establish the methodological approach used within the group;
- coordinate the whole process among subsidiaries;
- own and design IT systems and tools supporting the integrated Risk Management activities;
- consolidate findings and manage all reporting activities; and
- assess risks that affect the entire group, from a global perspective.”

The result can be, as in another airline, a risk register with over 400 different risk items that, after proper evaluation, analysis, classification and escalation, are prioritized so that the board of directors looks at the top 20 risks only.

A different example shows that an airline has several risk categories: A, B, C, D risks which also enable escalating or delegating risk management decisions up or downwards in the organisation. The Board of Directors takes care of all A-rated risks. This airline also evaluates each risk (and each risk category) differently, as it considers that each risk has its own lifecycle, somewhat comparable to product lifecycles.

The airline that chose a more quantitative approach states that, because of their approach, “we are getting improved feedback about the risk sensitivity of 12-month cash flow.” There is a quarterly registration of current probabilities and the monetary loss of an event and then the same evaluation after responding with risk limiting or mitigating actions.

One interviewee, from an airline using ISO 31000 as their guiding standard, was kind enough to show the actual tables produced during the risk management process, demonstrating that the ISO 31000 standard actually works. It was possible to see all information on risk identification, root cause analysis, risk evaluation, mitigation measures, net risk levels and even a global risk map. This was the proof that more than being a theoretical exercise, it is possible to apply all ISO 31000 suggestions into the airline business. Currently all layers at this airline are familiarised with the process and contribute actively, by feeding the risk register and participating in the regular risk workshops and meetings. This airline’s representative stated that while it took about three years to achieve this level, their next step is to define and quantify their risk tolerance level, the so called risk appetite.

Unfortunately no other airline representative showed how their approaches were translated into reality, by sharing or just displaying screenshots of tables and documents.

In any case, the actual approach an airline chooses for its risk management depends a lot on the appetite it has towards risk, either more averse or prone to accepting them.

In one case, the Board of Directors together with the Risk Management Committee defined the generic guideline for risk appetite, which is translated into a yearly quantification of acceptable risk.

“This does not mean that risks with impact beyond that level are discarded and not looked at. Some are not avoidable (e.g. fuel price increases) therefore have to be managed responsibly in and by the organisation. They are escalated to and discussed at a higher level within the organisation, such as the Board of Directors, deciding how to handle that item.”

Another similarly large airline tends not to follow the same path on defining and quantifying a risk attitude, preferring not to have a formal definition or value, given that the business is so closely linked and dependent on the countries’ GDP performance.

A third airline representative rejects completely the need for defining such a risk attitude as it is “an irrelevant exercise with no importance”. If an event occurs, it has to be dealt with regardless of being above or below any theoretically defined level. Each event might trigger other events that have not been considered beforehand.

An additional interesting comment came from another airline executive, as answer on how to manage risks that are beyond the airlines’ control, thus not manageable by the airline or not even insurable. “Those might include only political risks or risks that can be handled by authorities. Depending on the level of the required solution (i.e. CAA/Ministry of Transportation, Government Decrees or Parliament laws) the top managers responsible for liaison with the appropriate authorities are required to communicate and search for a solution. Such a communication most often is arranged via membership in different business organisations. [...] If the above approach is not enough then shareholders are working at the highest level of country's decision makers”. This shows that in some cases high level lobbying is still a way to solve such issues.

5.3.3. Organisation

It has been seen before that some airlines tend to follow a more centralised, others a more decentralised approach to risk management. Some use bottom-up approaches only – where risks are thoroughly identified by lower line management and individual business units, consolidated and reported upwards until the various filters select the key risks that go to board discussions. Some others use top-down approaches only, attempting to involve top management from the early stages of key risk identification and detection of mitigation measures. In this case, lower ranked issues are supposed to be handled by the respective functional department or business unit.

One airline stated that they used to have a bottom-up approach only, but now this has been complemented by a top-down exercise, too. This top-down commitment is made visible as the risk group, which oversees the work, is composed by the CEO, key directors and the head of Enterprise Risk Management, showing a clear involvement of upper management layers. “This meant no-one argued with it or tried to avoid it. Everyone was doing it.”

Another airline, despite having a centralised risk management function, sees this unit more as a risk champion within the airline, conveying the message and importance to manage risk within all functions of the airline. Every manager is still responsible for managing their own risks. There is a centralised register for some areas of business, although some do not contribute as key risks don’t change significantly from time to time. There is a Risk Report that goes to senior management and board every 6 months highlighting key risks, emerging risks, how they move, etc. When asked about the success of this model, this airlines’ representative stated that the success is visible in the daily business as the company keeps on growing and facing competition with innovative and well accepted products, without negatively impacting the airlines’ bottom line.

A smaller airline shows a less complex organisation. There is a small central unit taking care of risk and insurance, handling mostly insurance contracts. They do not establish standards and templates for risk management as it is Internal Audit that assesses risk and risk management. According to the airlines’ representative, there is no systematic way of deciding a risk appetite threshold, at least for commercial risk. In such a small organisation, size of management helps: it is easier to discuss issues and get things done.

When it comes to the integration of risk management with internal audit functions, several contributions were once again received. One airline stated “these are separate due to the different nature of their fundamental responsibilities. A crucial point is the primary role the internal audit has in independent surveillance and control”, therefore also surveying the risk management process.

Other airlines tend to integrate both functions, and yet another shows varying organisational patterns over time: risk management was sometimes integrated with internal audit, on other occasions it was separate and reporting to the airlines’ Chief of Staff or Company Secretary.

This shows the existence of various organisational models for individual airlines. How does it work with merged entities? One airline shares their experience, after the accomplishment of a merger process. The parent company gets input from the individual airlines separately and puts everything together in the corporate risk model. Nevertheless, each airline has their own models and risk registers, and might even have different views on the same risks. As geographies, local economies and social aspects are significantly different, key risks for each respective organisation might also differ significantly.

In terms of speed of implementation, one airline risk manager mentioned a few years to change cultural and communication aspects within the airline to make the process flow smoothly. Another risk manager stated “implementation and regular data collection has been slow. The internal audit [department] and I consider it a long term goal to change the risk culture and improve the in-house perception for the task but admittedly the project has been seen as a bureaucratic step and that has been a drawback”. It must be said that this airline in particular stated a very quick implementation (from nothing to sophisticated tool usage) in less than six weeks of introduction of a software solution, on which training and user meetings were held during one year to test functionalities and eliminate difficulties.

Therefore also relevant for organisational issues is the support (or not) by a software solution and automatic tools.

One large airline representative said “[we] implemented a standard IT software solution that is partly configured to our requirements and enables the constant follow up, editing and revision of individual risks and facilitates the reporting processes by having a number

of standard reports that can be easily generated by from the tool. Different combinations of evaluation parameters can be used to extract deeper information on individual items."

Another airline interviewee stated that they "consciously haven't taken somebody else's model", but built their own and evolved it internally.

Despite all above, a third airline representative preferred to keep things simple and work only with spreadsheets that everyone could handle. The tool should not be a hurdle, scaring people away from the risk management process – that is already complex by itself – or delegating it to someone else. The easier people can contribute, the better.

5.3.4. Other topics

As stated earlier, cooperation among airlines on topics related to risk management is apparently non-existent. At an alliance level, all interviewees rejected the possibility of discussing such issues with partner airlines as these might constitute legal challenges to the alliance. But also from one individual airlines' perspective, it has been fully rejected to discuss risk issues with fellow partner carriers as there is no apparent value in doing it. Another representative stated "cooperation is within the authorities mentioned but not much with other airlines as I know of". IATA's working group on risk management is unknown to the majority of the interviewees.

Further on, one former risk manager of a large airline stated that the success and sustainability of their risk management process was affected by the change of CEO's with new/different perceptions of its importance. While one CEO was very supportive of the idea, boosting the organisations' openness and capabilities to introduce risk management, his successor seemed to slowly let things fade away, not giving as much importance to it.

When asked about the reason for this change in attitude – and also for the repetitive nature of risk management (the same things keep happening again), the answer was "people are people, they don't learn or don't want to learn or there is lack of handover in succession planning". Risk management can be seen as contribution to knowledge transfer, but it depends on how strong the risk coordinator is in the company. A risk manager should be seen as a middleman between conflicting departments so that issues are debated and discussed openly, not contributing to a stage of 'no action' and negligence.

5.4. Contributions from supporting activities

As mentioned in section 3.2 above, during the work package description, a number of supporting activities such as training courses, conferences and seminars were attended to provide even more background and content on how airlines manage risks. The three initiatives that stand out are the following training courses:

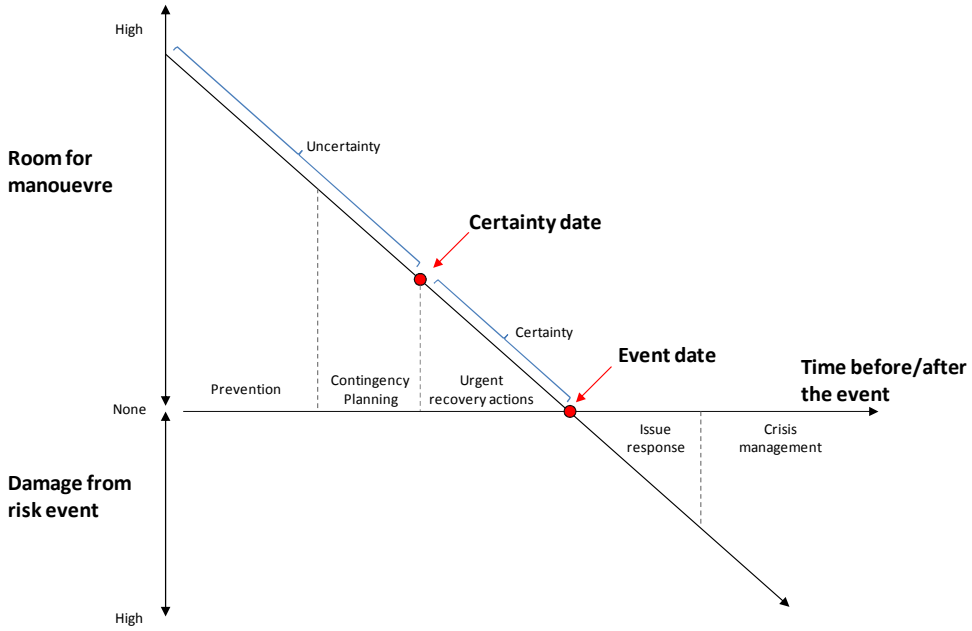
- Aviation Risk Management, provided by the Air Business Academy (an Airbus subsidiary) attended in Toulouse in October 2007;
- Aviation Risk Management using ISO 31000, provided by Aerosafe Risk Management and the Airline Industry Association of New Zealand, attended in Wellington in November 2012 ; and
- Risk Management Foundations, provided by the International Air Transport Association attended in Singapore in May 2013.

While all three courses revolved around the same subjects, risk management at airlines, they had fundamentally different approaches and contents, each providing interesting contributions to the thesis and showing ways how airlines can manage risk (in two cases using ISO 31000 as guiding standard).

When the first course was attended, ISO 31000 hadn't been published yet. Also COSO was still quite recent and not yet widely used by airlines, therefore no references to any of these standards were made during that course. Focus was set on financial risk management topics, exploring quantitative tools and methodologies such as hedging instruments for commodities, currencies, aircraft valuation and leasing agreements, insurances, etc. all while presenting case studies on how airlines manage risks (Iberia and Southwest Airlines). Operational risk management was addressed from a very high level perspective only.

One interesting aspect referred to the definition of two dates in operational risk management: the certainty date and the event date. The certainty date is "a point in time, normally some time before the event date, when it is clear that the risk is almost certain to occur and must be planned for". The event date is "the point in time at which the risk or condition will either occur, or the danger of occurrence will have passed" (ABA, 2007). Graphically this is depicted as follows.

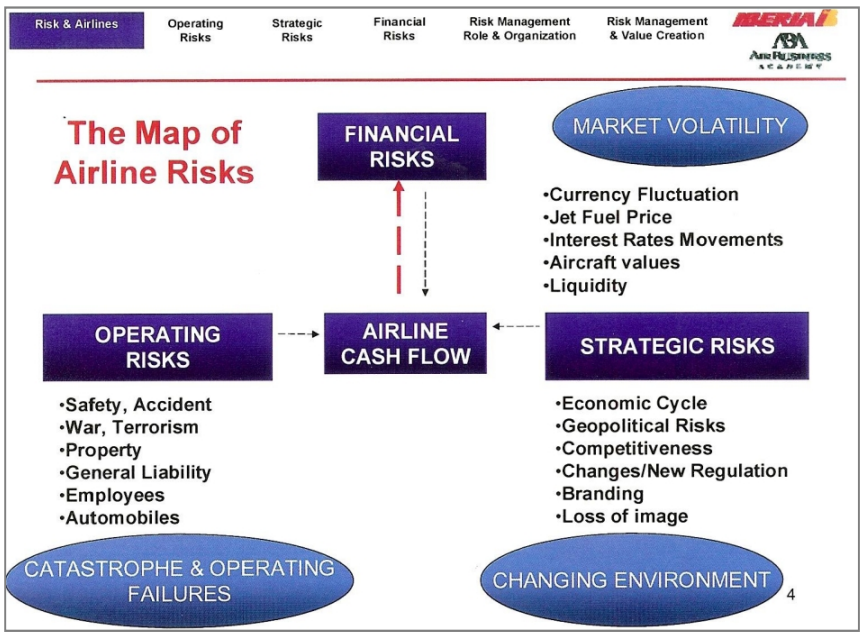
Figure 80: Certainty date vs Event date



Source: (ABA, 2007) adapted from Rachael Puchercos-Docherty

The Iberia case study was presented by Iberia's Finance Director, and structured around their view of an airlines' risk map. Therein the airlines' cash flow seems to be the centre and core of all risk management activities: protecting cash flow to keep the business running. There are three types of risk that have an impact on the airlines' cash flow: financial risks, operating risks and strategic risks.

Figure 81: Iberia's Map of Airline Risks



Source: (ABA, 2007), IBERIA Case-study

The financial risks can arise from market volatility and unforeseen fluctuations in commodity prices. This includes currency fluctuations, fuel price variations and interest rate movements, among others. The operating risks relate to the actual business operation: accidents, political issues (wars and terrorism), property damage, general liability, etc. These are all events that result in catastrophic and operating failures. The final risk type relates to strategic risks arising from a constantly changing environment. Examples include the economic cycle, geopolitical risks, competitiveness and regulatory issues, as well as branding and image issues.

Given that this example was presented in 2007 it is assumed that Iberia already changed their approach to risk management (as seen in the annual report survey presented above).

As for Aerosafe's course on Aviation Risk Management, this was the first more practical training on how to apply ISO 31000 to the airline environment. The course started by separating the three different types of risk and the applicable management plans to each:

- Uncertainty-based risks are handled by business continuity planning, recovery planning, crisis management and emergency preparedness.
- Hazard-based risks relate to safety, occupational health and safety, operational risk profiling (e.g. environmental risk, operational risk, etc).
- Opportunity-based risks require venture risk management and change management to assess the up and downsides of risks.

According to the trainer, ISO 31000 can be applied to all situations, although the training focussed more on using it for the opportunity-based risks and how to develop a venture risk management plan in the airline business, such as a new route, a new business, etc.

The concept of aviation governance (defined as "the system by which organisations are directed and controlled") was presented as being composed of three elements:

- Compliance, with all national and international, industry specific and industry neutral laws and regulations around the companies' activity;
- Assurance, making sure the company has proper insurance coverage for potential events causing material and immaterial damage; and
- Risk management, preparing the organisation to face events.

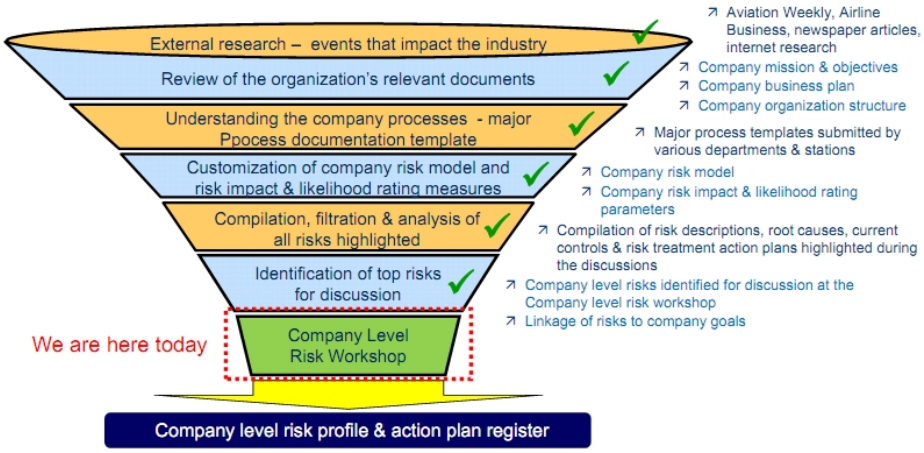
The rest of the course revolved around ISO 31000, its components, application techniques and explanation of some risk management templates. Aviation examples were provided by participants who were then invited to apply the risk management templates provided by the trainer to the various examples mentioned. Participants came from all possible areas of

aviation: regulators, commercial airlines, emergency air transport operators, rotor-wing operators and consultants.

While being similar in content, the Risk Management Foundations course provided by IATA was much more linked to the commercial airline business, as also most of the participants were coming straight from the member airline community. Therefore examples and discussions were directly related to the content of this thesis. The course followed the IATA Integrated Risk Management Manual (IATA, 2010), as presented and discussed earlier, therefore no new definitions or applications were apprehended. Nevertheless, the course was valuable in seeing and hearing practical experience on applying that model, covering most soft aspects of developing and implementing a risk management process. One of the most relevant topics was the discussion around a risk management workshop: its contents, preparation and execution, as well as importance in defining the companies' risk profile and action plan.

The preparation includes a thorough review of internal and external information, gathering organisational process description, organisation charts and responsibility descriptions to prepare risk process templates. Major risks for discussion should also be identified, assessed and evaluated beforehand.

Figure 82: IATA Risk Management Workshop Preparations



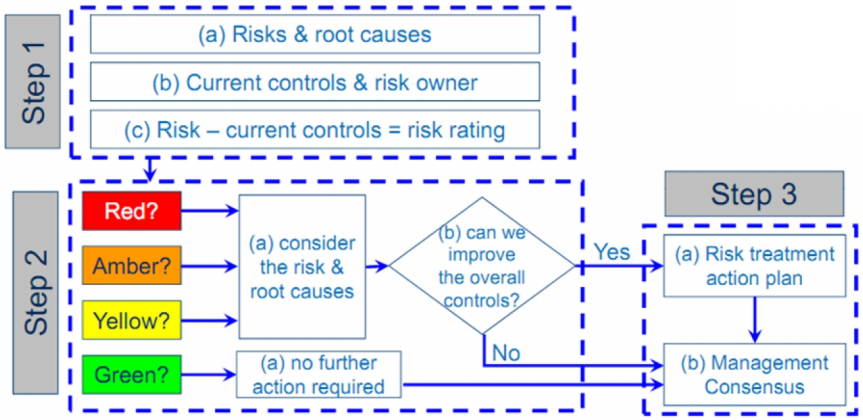
Source: (IATA, 2013b)

Such a workshop should be conducted in three steps:

- Step 1, to discuss key risks, their description, root causes, controls and control effectiveness;

- Step 2, to rate risks according to predefined criteria, map them in the organisations' risk landscape and check if further actions are required; and
- Step 3, to address potential risk treatment plans and get management consensus on these plans.

Figure 83: IATA Risk Management Workshop Steps



Source: (IATA, 2013b)

5.5. Chapter summary: key findings from the research process

It is clear that there is no uniform approach to risk management at airlines, despite the widespread availability of national, international, and even industry-specific, risk management standards.

As shown in the previous sections, the actual use of risk management and the reporting thereof seems to be quite divergent: 29 airlines didn't publish regular reports for the Financial Year 2011 and/or don't include any statements on risk management in their reporting; another 32 airlines refer to some risks they are exposed to but do not mention any specific standard used as guideline for their risk management activities. It is not possible to judge if these 61 airlines have or don't have formalized risk management practices in place, although at some companies the interviews conducted (notably British Airways, part of IAG) suggest that not all is being publicly reported. Most North American stock-listed airlines, and a few from other regions, totalling 28 airlines, have statements citing COSO as guideline for internal control activities – but the majority does not show how COSO is applied for the actual risk management activities.

On the other hand there are few airlines that show very advanced risk management models, being quite transparent in the way this is reported. Qantas, Lufthansa, Cathay Pacific or TUI Travel are examples. Two airlines cite AS/NZS 4360 (now upgraded to ISO 31000) and just six airlines referred to ISO 31000 in their 2011 Annual Reports.

The interview process showed different views on what the context was in which airlines introduced their risk management approaches. Topics such as the process structure and the organisation of the respective risk management units were also addressed. Following can be listed as conclusions thereof:

- Interviewees stated that company-wide risk management is a lengthy process, requiring time, resources (money and skilled staff) and top management support to be successful. Most airlines do not have this readily available, let alone a deep understanding of the risk concept itself, therefore holistic risk management is not an easy and straightforward task every company can quickly implement.
- Operational risks are traditionally well covered, mostly due to regulatory and compliance reasons, but other risk areas are weakly covered. Some airlines tend to misinterpret risk management as insurance management, therefore think that by having the latter, they are covered for all sorts of risks – including those that are not insurable.
- Because the above requires a fundamental culture change within the organisation, setting up a company-wide and holistic risk model requires a clear vision and milestones for its implementation. The example from Garuda Indonesia, shown in section 5.2.3 above, covering a four-year period for their ERM implementation matches these statements.
- That risk management is an area with limited cooperation among airlines, as seen earlier by IATA's lack of success in gathering input and support for its own attempt to introduce an industry-specific risk management model, has also been quoted by airline representatives during the interview process. Risk and the management actions taken to tackle them are – strangely – mostly seen as sensitive issues to the airlines' businesses. As this is a key area for criticism, cooperation among airlines and relevant stakeholders shall be included in the framework adaptation for a true company-wide risk management effort. (There are plenty of areas where airlines cooperate at bilateral or even multilateral levels, so sharing information on how to tackle risks that all airlines face should be of mutual advantage, not used as competitive weapon.)
- In terms of process used, several views could be collected: from a "keep it simple but effective" approach to a rather sophisticated version using quantitative modelling to calculate financial impact of every identified risk. While it is clear that there is no single way to do risk management, the airline should choose the way it feels most comfortable with as long as that helps it achieving its goals.

- Although stakeholder management has been listed by many interviewees as a key element in the risk management process, few airlines show this as being part of their risk management approach. Cathay Pacific is very transparent in this respect and shows the stakeholder management features in the publicly available reports.

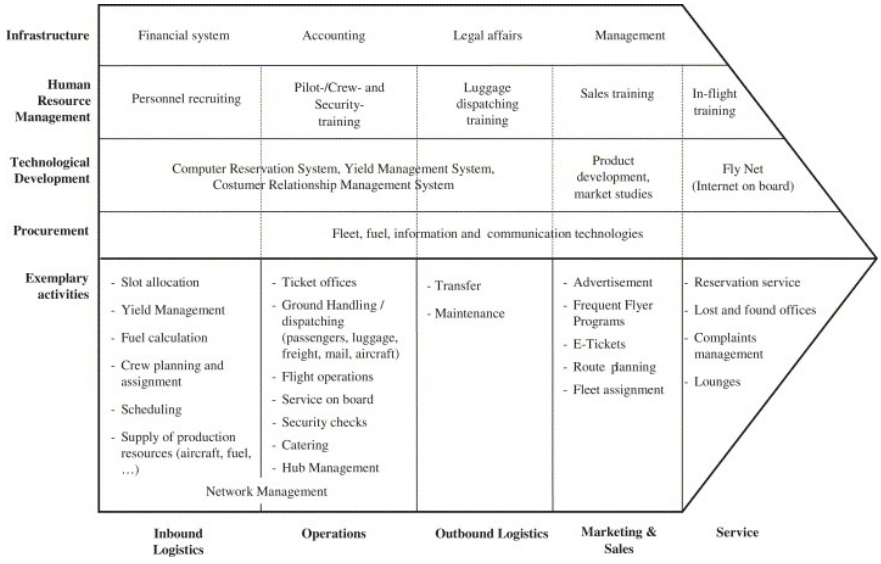
From all this, there are at least two immediate questions that arise:

1. Why is there a limited use (or reporting) of risk management practices?
2. Why do so few airlines use ISO 31000 or can ISO 31000 be used by airlines?

Potential answers to these questions will be discussed in the next chapter.

What is also surprising is that several academics (Albers, et al., 2005) and industry analysts have never included risk management as a separate process in a typical airline value chain, while other management and specific processes (such as accounting, logistics or marketing & sales) are all represented. Is the subject not relevant enough? Is it already included in a wider topic? Or should risk management not be considered a process for inclusion?

Figure 84: Typical airline value chain



Source: (Albers, et al., 2005, p. 50)

The corresponding author of the paper where the Airline Value Chain depicted above was published has been contacted and he now states “risk management is a highly important topic for airlines, and it needs to be a top priority among airline managers.”[18] How risk management can be integrated into the value chain will also be seen over the next chapters.

[18] Based on an e-mail exchange held in August 2013.

6. Discussion and identification of improvement areas

The previously exposed work led to the identification of current risk management practices at the largest airline groups – or at least the way these airlines report on those practices. This chapter will critically discuss these findings in an attempt to identify improvement potentials on how to introduce better risk management at airlines. To support this, some core issues within the airline industry will be looked at, while also discussing contributions from other industries on their risk management practices.

6.1. Critical issues

This section will discuss possible answers to the two questions listed earlier:

1. Why is there a limited use (or reporting) of risk management practices?
2. Can ISO 31000 be used by airlines?

This will be then followed by reasons to keep ISO 31000 as guiding standard.

6.1.1. Limited use of risk management

Based on replies received during the interview process, it is possible to list a number of reasons that can potentially justify why the use of risk management – and ISO 31000 in particular – is not as widespread as expected. They include:

- Lack of leadership and commitment.
  One interviewee stated that the change of CEO's at the airline led to a deviation of focus and thus less attention was given to risk management. While the previous CEO was a very enthusiastic supporter, his successor concentrated efforts on other activities, with risk management losing importance. On the other hand, airlines that have stated strong commitment to risk management by upper management levels have been successful in introducing the process and getting the buy-in of all involved employees.
- Lack of knowledge and understanding of concepts.
  Risk and risk management are concepts that require a significant time for maturation and understanding. The associated standards, principles and guidelines are not easily grasped and need to be applied to the specific industry and company. Moreover the whole concept and company approach need to be communicated, disseminated and lived by the entire organisation.
- Lack of interest and/or other priorities.
  A company that has too many priorities cannot dedicate all available resources towards their achievement: some will not be achieved. If risk management is not supported and communicated, interest cannot be created and awareness risen.

- Lack of resources (financial, human, technical, time).
  Without resources, little can be achieved. If an organisation decides to embark on an activity, it needs to be able to do so. If resources are not available, no risk management – or any other activity – will ever materialise.
- Lack of proper and/or industry-specific guidance material, and/or acceptance of existing material. Templates and forms are sometimes not available, needing significant time and effort to be designed. Guidance material is sometimes dense and not user friendly, thus not helpful in implementation exercises. Hiring external consultants to develop such templates, design the whole process or help during the implementation phase is costly and sometimes not effective, as knowledge doesn't stay in the organisation and gets diluted with the consultants' departure.
- Lack of training on tools and techniques.
  Sometimes organisations tend to solve problems by acquiring a tool. While tools are normally helpful, they should not be an end by themselves. One interviewee fully rejected the use of over-sophisticated tools, suggesting the use of simple Microsoft Excel and Word tables and forms. But if the organisation decides to acquire any tool, training should be part of the package. In any case such training is only effective if the recipients are also willing to learn. Sometimes a natural opposition to change blocks any attempt for improvement, even with tools.
- Seen as another bureaucratic hurdle.
  Risk management can be viewed as just another bureaucratic effort, forcing the filling of tables, forms and templates, attending lengthy meetings and potentially even involving hearings at upper management levels. The language used throughout the company needs to be harmonized, so that all involved understand themselves when referring to 'risk' or 'hazard'.
- Internal and/or external opposition.
  Because of the above, internal opposition to the introduction of such a new process can easily arise and its implementation be boycotted. Getting the buy-in of internal staff, middle or upper management, or even the support of external entities such as the board of directors is therefore essential if the organisation wants to implement it successfully. Imposing in a top-down manner, using force and blame is not the right way to do it; rather the opposite, using a positive dialogue culture, hearing peers and incorporating input received.
- Lack of cooperation between industry bodies.
  The airline industry is a great example of cooperation among players at formal and informal levels. Several issues are commonly discussed among peers – notably safety-related ones – without putting in danger competition and anti-trust rulings. Sharing experience in risk management, at least at a process level, should help airlines overcome initial hurdles and difficulties. IATA has such a discussion group, but unfortunately none of the interviewed risk managers knew of its existence, let alone participate in it.
- Time intensive exercise.
  Yes, risk management will take a lot of time and resources. Day-to-day business normally takes up most of the time, thus loading the middle and higher

management with an additional burden of meetings, forms, decisions and explanations easily adds to the opposition to such a process. Also, as it requires a culture change within the organisation, one interviewee states that a full implementation of a risk management process might take up to five years.

- Voluntary nature of risk management.
  An enterprise-wide risk management process is not required by any national or international regulatory entity, therefore it is seen as an optional management decision. Also, and unlike other ISO standards, ISO 31000 is not object for certification, adding to the voluntary feeling of the whole process.

The list is certainly not complete, but it is possible to summarise all the reasons in one simple statement that could by itself justify the limited use of risk management: limited visibility of results. If the results of risk management were largely visible and quantifiable, the topic would get all attention, resources and commitment from upper management, involvement from middle managers and endorsement from the board of directors. But results are not that visible.

And yet there are companies that still introduce risk management processes. One example is the SATA Group (an airline group based on the Azores islands in Portugal, with interisland, mainland and intercontinental services) that in the year 2012 decided to introduce a COSO-based risk management approach. While it is still too early to judge if results are as expected, the airline chose to use COSO instead of ISO 31000 (despite it being more recent), because it seemed “more complete and, above all, more consolidated”[19].

So, given the limited use of ISO 31000 as proven during the interview and survey steps, and this recent statement by SATA, is ISO 31000 applicable to the airline industry?

[19] Based on an e-mail exchange with the respective project manager in August 2013.

6.1.2. Can ISO 31000 be used by airlines?

As seen earlier, ISO 31000 has been presented in 2009 after a long period of maturation and discussion among risk management specialists and member states. Some airlines – very few – have successfully used it as guideline for designing and implementing their own risk management. Nevertheless it is clearly not the first choice, even for airlines that have recently started introducing risk management practices.

At the same time, the Chair of the ISO working group for risk management and lead author of ISO 31000, Kevin Knight published an article about ISO 31000 and the 2010 Icelandic volcano crisis where he states "surprisingly such an event does not appear to have featured as a risk that airlines and many other companies needed to manage. [...]Some would suggest that the havoc was caused by a failure of risk management, rather than the failure of Boards and top management to effectively manage risk." Further on he says "ISO 31000:2009 is clearly different from existing guidelines on the management of risk in that the emphasis is shifted from something happening – the event – to the effect of uncertainty on objectives" (Knight, 2010, p. 1).

Some years have now passed since the introduction of this standard and yet it still lacks adherence by airlines. Thus Mr. Kevin Knight was invited to answer two questions:

a) Can ISO 31000 be successfully used at airlines? and
b) Why do so few use ISO 31000 and when they do, not all risks are covered?

His answers couldn't be clearer[20]:

a) "Most emphatically yes as ISO 31000 is focused on the achievement of objectives by making the correct decisions and all airlines have objectives to achieve - safety; market share; competition; regulations; etc. Qantas is an excellent example of an airline that effectively manages its risk as an integral part of how the company is managed."
b) "The fact that some people only associate risk with insurable loss limits how they think and they therefore do not read ISO 31000 as they assume it is for their insurance people. To overcome this historical assumption, that risk management is all about insurable loss, we use the term "management of risk" with an emphasis on the fact that every time a "risk owner" exercises their delegation to make a decision, with respect to a particular matter, they create the risk of 'have they made the right decision' and 'can they manage it to a successful outcome'. ISO

[20] Based on an e-mail exchange held in July 2013.

31000 is about management and is why it has now been picked up as a component of Management System Standards."

But despite the limited use, there are airlines successfully using ISO 31000. Beyond the Qantas case, South African Airways is another good example. During the face-to-face interview conducted with the Chief Risk Officer of South African Airways, a step-by-step demo of tools and templates was performed proving that ISO 31000 can be applied.

Therefore, to help more airlines introduce risk management using ISO 31000, this thesis will propose a redesign of its application framework, making it more specific to the industry, rather than proposing a radical new process or model. This framework shall bring ISO 31000 closer to the airline environment and thus help airlines introducing risk management practices into their organisation.

6.1.3. Reasons to use ISO 31000 as guiding standard

Given that ISO 31000 is clearly not the most popular option when it comes to airline choice for a risk management standard, why should this be kept as guideline for any further development effort? Why not COSO?

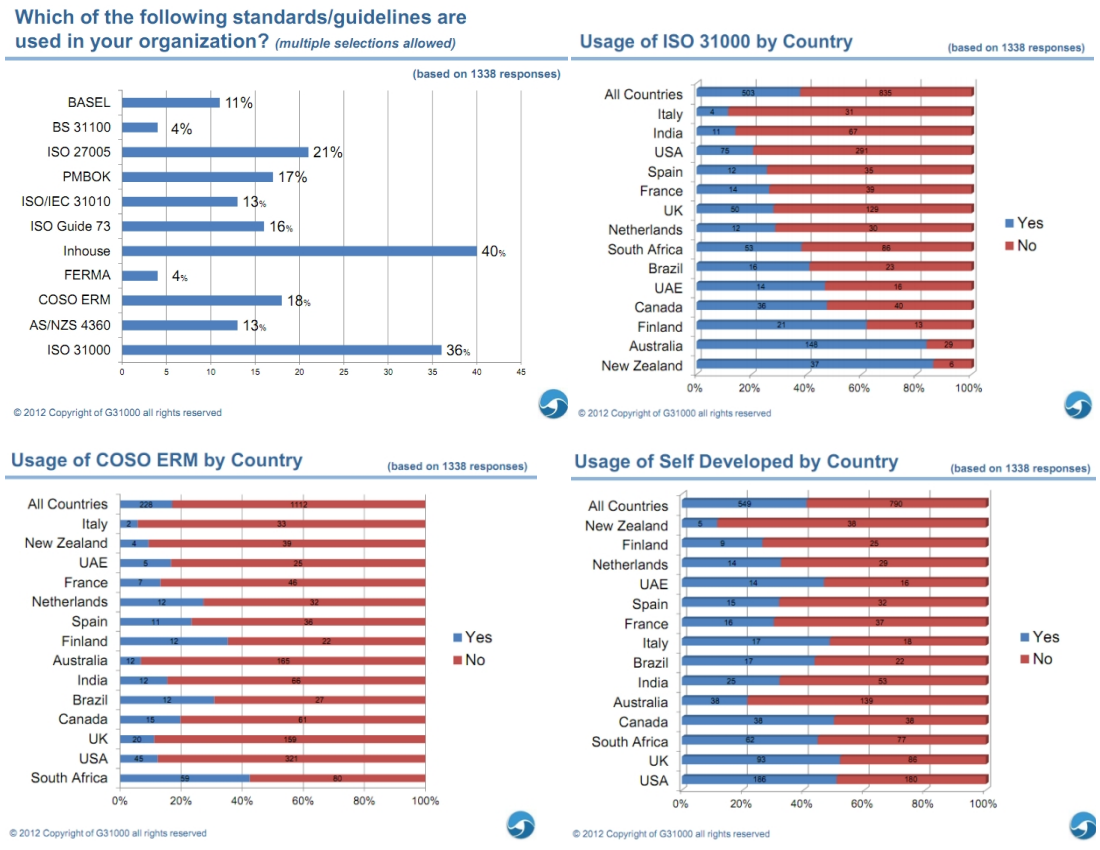
There are several independent reasons that justify such a decision, all sourced from the conversations and interviews conducted. They include:

- ISO 31000 is the most recent standard. The IATA model has been published one year later, but it hasn't been accepted: none of the surveyed airlines list it as the standard of choice.
- It is the only internationally valid and recognized standard, with already over 40 countries recognising and adopting it as their national standard for risk management (G31000 Global Risk Management Platform, 2012).
- It is industry neutral and has been implemented in many industries, geographies and company sizes.
- It can be flexibly adjusted to the airline environment (or any other industry).
- Some airlines have already successfully applied this standard.
- ISO 31000 enables a holistic view of risk not only inside the organisation, but also in its environment.

At least two surveys have been conducted by independent organisations to understand if and why ISO 31000 is preferred over COSO, and what the respective reasons are. The Global ISO 31000 Survey published in 2012 by the G31000 Global Risk Management Platform (and presented during the first ISO 31000 Conference held in Paris on May 21st-22nd 2012) shows that 44% of 1086 respondents (risk practitioners from 111 countries and

all possible industry sectors) say ISO 31000 “is a significant improvement” over other risk management references, guidelines and standards. 40% say “it is quite similar” and just 2% say “it is worse”. When asked about which other standards are used within their organisations, an apparent tendency to use in-house developed tools is visible, with 40% of all participants referring to this option. A further 36% cite ISO 31000. Nevertheless, other documents related to ISO 31000 such as the ISO/IEC 31010 and the ISO Guide 73 are quoted separately on this list, so that the global outcome might still be favourable to ISO 31000. Surprisingly COSO is just quoted by 18% of respondents. Unsurprisingly, from a regional perspective, ISO 31000 is mostly used in New Zealand and Australia. What is surprising is that COSO is mostly used in South Africa and that the most used risk models in the USA are self developed ones. (G31000 Global Risk Management Platform, 2012)

Figure 85: G31000 2012 ISO 31000 survey results



Source: (G31000 Global Risk Management Platform, 2012)

From a more qualitative perspective, a survey conducted by Norman Marks, a veteran risk practitioner, shows other also interesting results (Marks, 2012). He asked about 180 other risk practitioners if they explicitly preferred ISO 31000 or COSO and why. 52% preferred ISO

31000, 15% opt for COSO and 25% state that they have no preference as "either can be used effectively". The reasons listed for or against each of these choices are listed below.

Figure 86: Norman Marks survey results ISO 31000 vs COSO

"Those who prefer ISO 31000:2009 offered these opinions: • Easier to understand and explain to others. User friendly. • Written by practitioners instead of accountants and auditors. • Clear, logical, intuitive, and practical. • A better 'how to' guide, easier to use when implementing risk management. • More focused on risk and less on audit and controls than COSO. • Represents best practice and the collective wisdom of global risk leaders. • Flexible, less prescriptive, easily tailored. • Has a top-down approach to risk management."	"The people who prefer COSO ERM did so because, in their view: • It is comprehensive and has stood the test of time. • It is the standard that has been adopted by their regulators. • Their organisation previously adopted it. • It links to the COSO internal control framework. • It has a better discussion of risk appetite. • It is stronger on corporate governance. • There is a better linkage to strategies and objectives."

Source: (Marks, 2012)

Beyond the results of these surveys, ISO 31000 also helps tackling the possible reasons why risk management is not widely used:

- The first reason listed, lack of leadership and commitment, is tackled by the very first element of the ISO 31000 framework for managing risk 'mandate and commitment'. Herein clear tasks, goals, responsibilities and reporting lines must be defined by upper management so that the risk management unit can properly perform its duties.
- As for the 'lack of knowledge and understanding of concepts', 'lack of training on tools and techniques' ISO 31000 is the only standard that comes with supporting documentation, including vocabulary guidelines, Guide 73, and a document with tools and techniques for each process step, that can be quickly consulted for reference and guidance purposes. There are also several training organisations that offer dedicated courses to convey further tools for the implementation ISO 31000.
- The lack of interest and lack of resources mentioned above can only be addressed by the organisation itself. As soon as the risk management process shows results, interest will be created and resources allocated, so it is 'just' about having some patience to see the results materialise. The benefits of using ISO 31000, if well implemented, are clear and have been listed before.
- The lack of industry specific guidance material cited earlier is a fact and was one of the key drivers to pursue this research. When published, this thesis may act as further reference document for industry-specific implementation of ISO 31000.

- Internal and external opposition needs to be tackled by constant communication and consultation, as part of the ISO 31000 process. This may also lead to improved communication and cooperation among peers and industry bodies.
- By being quite detailed and proposing a stepped approach, ISO 31000 may actually reduce the time required to implement risk management; although it still won't be an automatic and quick process as seen during the interview process cited above.

Summarising: the wide-spread use, easier understanding and applicability, focus and tailoring possibilities justify the choice for using ISO 31000 as guiding standard for an airline-specific framework adaptation in the context of this thesis.

6.2. Key challenges

Related to the above discussion are two additional questions that, by themselves, could justify separate research projects. These questions are:

1. Is the airline industry resilient?
2. Is there a limit to growth?

Their pertinence is justified by the airline industry being, on one hand, probably one of the most exposed to external shocks, therefore requiring strong and thus resilient airlines, and on the other hand an industry that can only survive by constantly growing in volumes produced. Both elements carry risks with them, therefore any new airline specific risk management framework needs to provide tools for airlines to become more resilient and better prepared to face growth. The issues associated to these questions are briefly discussed separately below.

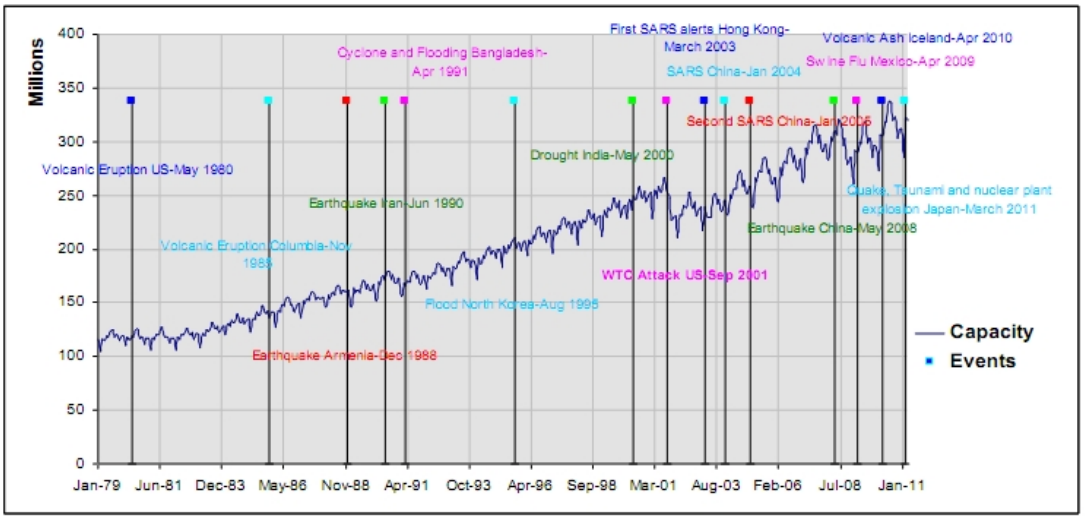
6.2.1. Is the airline industry resilient?

Resilience, as defined by Guide 73, is the "adaptive capacity of an organisation in a complex and changing environment" (International Organisation for Standardisation, 2009c, p. 11). There is no question that the airline industry is heavily exposed to such complex and changing environments. Michael Zea's typical airline risk landscape as shown in Figure 59: Airline Risk Factors, presents a number of externally driven risk factors that are beyond an airlines' control. How individual airlines as separate companies and the airline industry in general react to such factors has diverse interpretations.

A report by UBM Aviation analysing the impact of several "world crisis" events on the airline industry, comes to the surprising conclusion that "global capacity growth [by

airlines] is very resilient" (UBM Aviation, 2011, p. 13). The report analyses the impact of diverse events such as the New York World Trade Centre terrorist attacks in 2011, the SARS outbreak in China, the Swine Flu in Mexico, the Icelandic volcanic ash eruption in 2010, the Japanese earthquake, tsunami and nuclear plant events in 2011, the jet fuel price fluctuations over a 20-year period as well as the impact of the global financial crisis. In all these situations the authors come to the conclusion that the industry recovers well, although with different speeds depending on the type of event.

Figure 87: Crisis Analysis Chart 1979-2011



Source: (UBM Aviation, 2011, p. 4)

For truly global events capacity reductions are generally recovered after 12-36 months, regional events are recovered in a 3-12 month period and country specific events have an impact over less than 3 months.

The report produces several charts showing the evolution of global capacity after the occurrence of the respective events. The 30-year overview shows that, despite the number and diversity of all events, the global capacity deployed by airlines kept increasing. It is based on these elements that the above quoted conclusion on resilience is taken.

Critically speaking, this approach has two major flaws that make taking conclusions on resilience, as the one quoted earlier, a very risky exercise:

1. The report looks only at the impact of critical events on total capacity deployed by airlines, not the financial impact of these events or the sheer survival of the respective individual airlines.

There are a number of airlines that have suffered deep losses after, for example, the fuel price fluctuations in 2008, despite – or because of – their fuel hedging measures in place (e.g. Singapore Airlines or Cathay Pacific, as mentioned earlier). Others ceased operations after the occurrence of such events: Mexicana failed virtually immediately after the Swine Flu outbreak. Figure 53: Risk Management standards in the aviation context, shows just some of the failed airlines in comparison to significant events occurred in the same timeframe. Of course, no direct correlation can be taken (just) from such a depiction.

2. It is questionable if capacity is a good indicator of resilience, especially when considering the global airline industry.
   The industry is highly competitive and reductions by one airline leads to replacement of capacity by others that want to enter the market. Examples are the Brazilian airlines TAM and GOL that quickly compensated the capacity left vacant by the demise of VARIG, or the quick occupation by Ryanair and Wizz Air of space abandoned by MALEV in Hungary. Total capacity deployed in each market is thus quickly recovered – regardless of what internal or external events contributed to the failure of the established airline. It is therefore only natural that in competitive market environments strong airlines take over positions and market shares from weaker ones whenever they abandon. In monopoly or state controlled environments, the local airlines are protected (and possibly subsidised) by national authorities, thus financial hits might not be as relevant, even if deployed capacity is not efficiently filled.

Resilience is therefore something that each individual airline should be concerned with, from its own risk management perspective, in order to improve its resilience in uncertain environments. The global perspective is important, but the industry as a whole will certainly not help the survival of an individual airline in case of distress.

To support this, the CEO of a leading aviation risk and insurance brokerage company, Joe Plumeri at Willis Group Insurance, stated that “reputational risks such as skill shortages, currency or price fluctuations, or changing legislation are better dealt with by building resilience into a company. By having a risk management policy based solely on anticipation, a company will find that they are not fast or flexible enough to respond to a complex, interconnected and rapidly changing world” (Flightglobal, 2012).

This was probably what helped Icelandair cope with the volcanic ash eruptions in 2010. During this period, where most of European airlines had to cancel operations due to closed airspace, Icelandair managed to keep operating during the entire duration of the closure. One of its key decisions was to move the entire hub operation out of Iceland, from where it operated for 12 days. This decision was taken in just a few hours and implied moving 200 staff and its entire aircraft fleet to Glasgow. Icelandair’s CEO, Birkir Holm Gudnasson,

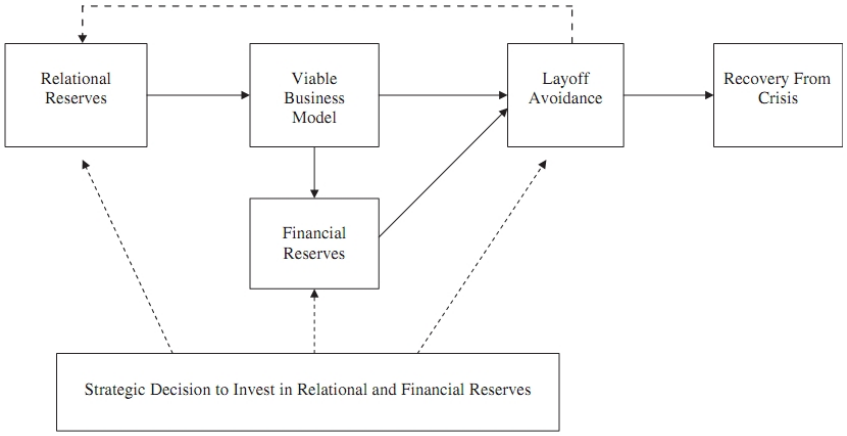
stated “if you are quick enough in your decision making and flexible enough, there are good business opportunities even in a crisis situation” (IATA, 2012b). This is probably the best example of how one airline showed resilience – understood as the earlier mentioned adaptive capacity of an organisation in a complex and changing environment.

In a different context, positive correlations have been established between airline resilience, relational reserves, business model robustness and financial reserves (Gittel, et al., 2006, p. 301). In this study, a mathematical model has been tested on results achieved by the 10 largest US airlines after the September 11 2011 terrorist attacks. The authors compare the independent impact of strong employee relationships, cash flow and debt levels, and an organisations’ business model (measured by the total operating costs per available seat mile) on their respective resilience, measured as the speed of the airlines’ stock price recovery to pre-9/11 attack levels. “By avoiding layoffs, [...] organisations maintain or even strengthen human relationships, creating coping resources that enable organisational members to respond cohesively to the crisis in innovative ways. [...]To avoid layoffs however, organisations must be financially able to do so. Financial reserves and viable business models thus play a significant role in minimizing layoffs and in sustaining the relationships that enable organisations to return more quickly to pre-crisis performance levels. [...] The most powerful implication of our model is that relational and financial reserves tend to be mutual reinforcing, forming a virtuous cycle that contributes to resiliency” (Gittel, et al., 2006, pp. 324-325).

Based on the results achieved, the authors expanded their initial conceptual model to include the “strategic decision to invest in relational and financial reserves” as a conscious management decision to foster long-term sustainability via strong employee relations and a financial cushion where both help the airline to recover from crisis situations.

It is of course questionable if this studies’ measure for ‘resilience’ (stock price recovery speed) can be considered valid, given the inherent stock market irrationality. A number of factors can contribute to stock-price increases or decreases; beyond the ones included in the model, some of them might not even be measurable for mathematical modelling purposes. In the particular case of the US-airlines, the immediate decisions by the US government to financially support airlines, notably providing guarantees for insurance policies in the aftermath of the 9/11 attacks, might have had equivalent impacts on the airlines’ stock prices. Stock prices are certainly never the result of one single factor.

Figure 88: Conceptual model of organisational resilience



Source: (Gittel, et al., 2006, p. 324)

What should also not be forgotten is that the airline industry is one of the financially least performing industries. A recently published report by the International Air Transport Association shows that over a 40-year period the airline industry has produced the lowest Returns on Invested Capital (ROIC) in comparison to 28 other industries (IATA, 2013d, p. 12). Additionally, in the air transport value chain airlines have not only the lowest profitability levels, but also the highest cost of capital (IATA, 2013d, p. 19).

Summarising this discussion, it can be said that the airline industry – understood as a single body – takes its time, but copes with external shocks, especially when this is measured by deployed capacity volumes only, despite low profitability levels. Such a statement cannot be made for every airline individually, as there are clearly lots of examples of failed airlines, therefore cases that were unable to cope with one or several such shocks.

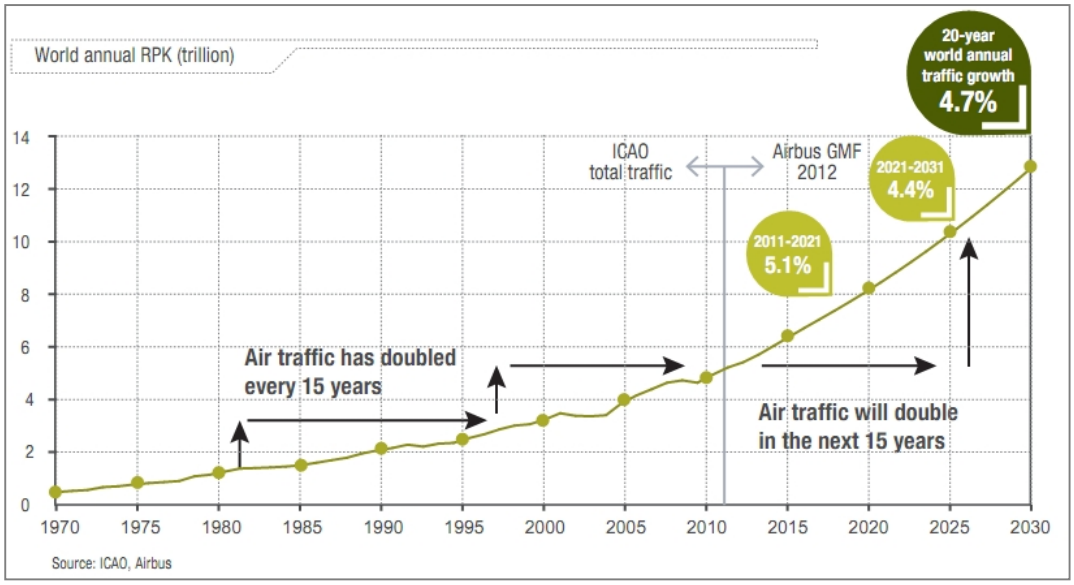
Because of this, all interviewees have been asked “when do you know risk management works?”, after respective processes had already been implemented. Most answers were vague, except for one (non-airline) risk manager that stated “the company keeps surviving!” alluding to the fact that the long term growth and survival of an organisation is an indicator of its continuous resilience to critical events.

How resilience can be built and incorporated into a risk management framework is thus a key challenge when adapting an existing standard to the airline-specific environment.

6.2.2. Is there a limit to growth?

The airline industry requires constant growth in capacity deployed and passengers carried. Historic figures show that not only does capacity keep growing (see Figure 87: Crisis Analysis Chart 1979-2011), but also that passenger demand duplicates every 15 years (Airbus, 2012, p. 52).

Figure 89: Evolution and forecast of global demand for air transport services, 1970-2030 [21]



Source: (Airbus, 2012, p. 52)

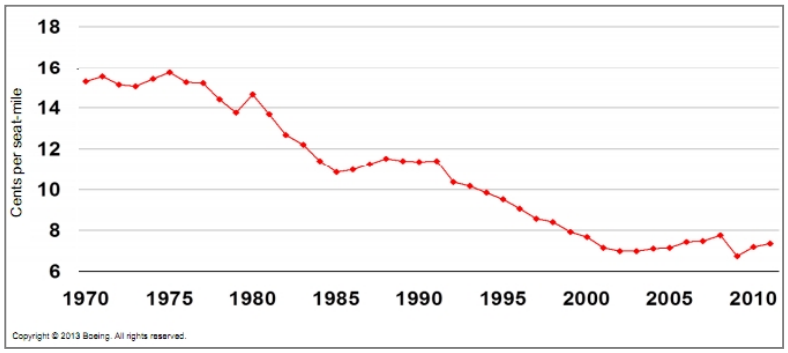
This need for growth comes not only as reply to increased demand. Of course, if more and more people want to travel by air – because they need and/or can – airlines need to be able to satisfy client requirements and deploy more capacity on existing or new city-pair connections. But at the same time, in an environment of constantly increasing costs (fuel, labour, technology, airport or air navigation service charges, etc.), intensified competition for market shares and falling yields, every airline has to conduct strict cost management to reduce unit costs of its production and compete more effectively against lower-cost airline providers or other – cheaper – modes of transport.

The tendency is clear: over a roughly 40-year long period yields (measured by cents per seat-mile, as indicator of the quality of revenue generated by airlines, see Figure 90: Evolution of global yield levels, 1970-2012) dropped 52%. Unit costs dropped at similar cumulative rates – or -2,3% per year over the 1980-2011 period. So while revenues per

[21] Measured in RPK (Revenue-Passenger Kilometres) as an indicator of demand for air transport services

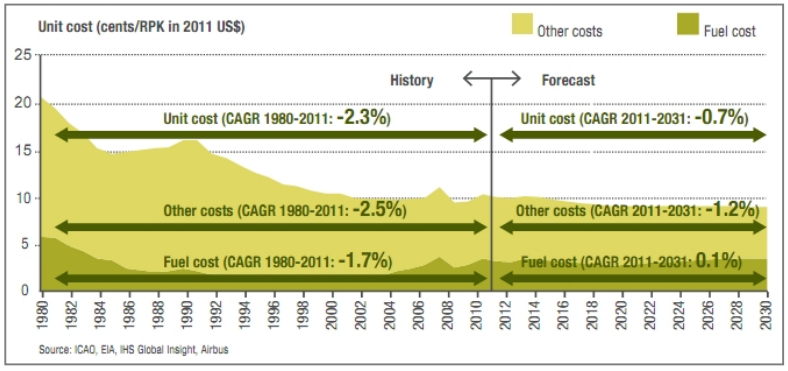
passenger-kilometre are falling (airlines are getting less money for more production) total costs are increasing; these can only be coped with by deploying more and more capacity, thus slashing global unit costs. Can unit costs be squeezed to virtually zero to match the continuous pressure on yields? Certainly not.

Figure 90: Evolution of global yield levels, 1970-2012



Source: (Boeing, 2013, p. 5)

Figure 91: Evolution and forecast of global unit cost levels, 1980-2030



Source: (Airbus, 2012, p. 52)

The problem is: how can this constant quest for growth be sustained and what risks are associated to such growth patterns. Putting this problem into the context of this thesis, how can each airline include sustained and sustainable growth into its risk management framework in order to cope with the inherent risks?

To match, fulfil and exploit such growth projections, pressure will be exercised on a number of issues, such as:

- Infrastructure – is there enough capacity available to accommodate more and bigger planes, both on ground and in the air? Mega-airports are already congested and have limited capacity for expansion; mature markets already have overcrowded airspaces. Of course, it is possible to rebate (part of) this argument

with the fact that the largest nominal growth is projected for less developed, so less congested, regions. But given that they currently also have limited infrastructure they will face the same problem, although at another level and with different implications. Growth remains the key issue.

- Labour – pilot and mechanic shortage is a problem some airlines are facing already today. Future growth will require more of these skilled labour forces, that not only cost a lot of time and money to train, but need to be retained within the companies as they are attracted by better-paying propositions from competing airlines.
- Capital – all these new aircraft, routes, staff, operating and marketing requirements require funding. Capital is not readily available everywhere and for everyone, let alone at affordable conditions. How are airlines going to fund these growth plans?
- Profitability – the above investments are necessary to fuel the companies' growth and expansion, but they will have a short-term impact on profitability levels in an industry that is already producing very low margins. How can the desire to improve margins be compatible with the need for further growth?
- Regulations – in deregulated markets there is virtually no limit to grow (as long as infrastructure allows, and even here the Single European Sky, for example, is far from being implemented), but in regulated markets traffic rights restrict growth. Moving on with deregulation towards full liberalization is a difficult discussion that some states and regions prefer to avoid or delay.

Extrapolating this debate, it would make sense to ask if there is – or should be – a limit to growth? This by itself brings additional questions and potential risks, that could almost lead to the failure of less-prepared airlines and therefore to more industry consolidation. While this is not necessarily bad – as least efficient market players would be eliminated – the emotions associated to the airline business, and protective character of some states, would stop take-over, merger or bankruptcy situations from happening, regardless of national or international rules in place.

Repeating a question asked earlier: how can airlines adjust? And how can their risk management framework cover all these issues, which are potentially of a very strategic and long-term level, but with daily impact on each organisation? An adaptation of ISO 31000 to the airline environment must therefore include means to address such high level issues. A risk management framework should not only be capable of addressing short-term and visible impact issues, but also enable the identification and discussion – at the appropriate forums – of broader issues as the ones mentioned above.

Looking back into what airlines include in their risk registers – or what they publicly report in their annual reports – the majority mentions only standard risks related to fuel price

fluctuations, currency exchange, credit and liquidity issues. Very few go into company specific long-term issues, of which Cathay Pacific is probably the best example.

Therefore, at this point it makes sense to understand how other industries are using and adapting available risk management standards to their specific environments, and how these capture both operational and strategic issues. The next section will address some findings of the research conducted to other industries.

6.3. Lessons learned from other industries

The interview process included visits to the risk management departments of two other companies from distinct industries: the largest electricity company in Portugal, EDP Energias de Portugal (since 2011 21% owned by China Three Gorges, one of the world's largest energy companies) and the largest telecommunications company in Portugal, Portugal Telecom (that recently announced merger plans with Oi, the largest Brazilian operator, creating one of the Top 20 global telecommunications companies). Goal of these conversations was to understand how these relatively large companies (both have multi-billion annual revenues and vast international operations) organise their risk management functions and check if any links can be established to air transport. Similar to the analysis performed for airlines, the annual reports of these two companies have also been consulted to review what is being reported in terms or risk and risk management. To complement this endeavour, as it was unpractical to visit companies from all sectors, a further evaluation of recently published surveys on industry wide risk management practices has been conducted. All findings are detailed in the sections below.

6.3.1. Utilities: EDP Energias de Portugal

EDP Energias de Portugal (from now on EDP) has been considered a global industry reference in terms of corporate sustainability and risk management. It has been successively awarded as industry group leader by the Dow Jones Sustainability Index (for the fifth consecutive year in 2013), an independent review of management practices at the world's largest corporations. This index combines a thorough analysis of industry specific and general criteria, revolving around an Economic Dimension (including risk & crisis management, corporate governance and code of conduct), an Environmental Dimension and a Social Dimension. EDP earned maximum scores (100) in the risk & crisis management section (DJSI - RobecoSAM, 2013)[22].

Moreover, over the years EDP has also been awarded with a number of other recognitions in the fields of risk management such as the Energy Business Gold Award 2009 for "Excellence in Energy Risk Management" (EDP Energias de Portugal, 2013c).

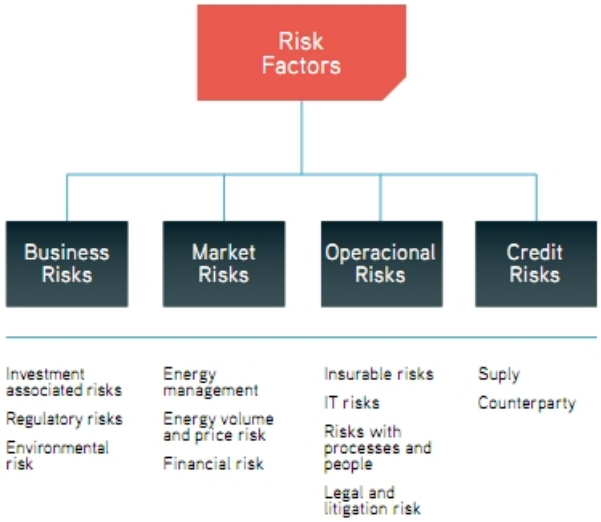
These are good reasons to look deeper into how this company is managing risks.

[22] In the transportation sector the leading company in 2013 is Air France, also achieving maximum scores in the 'risk & crisis management' category. Among all 25 airline contenders are Qantas, Lufthansa, Korean Airlines, All Nippon Airways, Cathay Pacific, Singapore Airlines and the IAG Group.

During the visit (in late 2009), EDP informed that their risk management model is based on an in-house developed tool that serves as a platform to centralize all risk events occurring in the companies' energy production and distribution, facility construction, corporate management, financing and all remaining activities of their business. Each subsidiary, business unit and even supplier nominates risk champions that are not only responsible for assuring proper risk management processes within the respective unit, but also to report all items into the consolidated risk database. At the time of the visit over 1400 individual items were mentioned and duly assessed. The function of the risk management team, in a bottom up effort, was not only to consolidate all this input, but also to filter according to pre-established criteria and escalate to upper management layers if and when required.

In the 2012 Annual Report, EDP depicts not only the group's main risk factors, but also a generic working mechanism showing what management layers have oversight over specific situations in the respective subsidiaries.

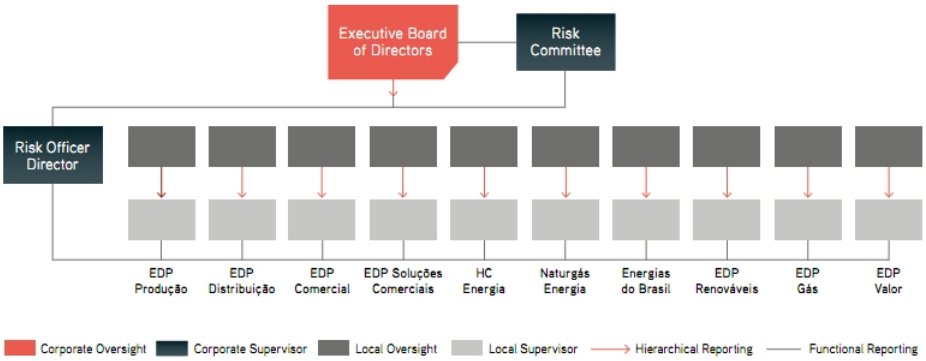
Figure 92: EDP Energias de Portugal group main risk factors



Source: (EDP Energias de Portugal, 2012, p. 118)

While the depiction of the main risk factors does not seem to bring any novelty, the description in the text of the Annual Report goes into much more detail – considerably more than in most of the top 100 airlines Annual Reports analysed. EDP shows that the company has a published risk management policy, how risk is integrated into their strategic agenda, what individual risks are, how these are being addressed and what key stakeholder issues are that can affect the groups' business.

Figure 93: EDP Energias de Portugal risk management organisation



Source: (EDP Energias de Portugal, 2012, p. 120);
Legend: EDP Produção, EDP Distribuição, HC Energia, etc. are EDP Group subsidiaries.

Starting with the integration of risk management into the Strategic Agenda 2012-2015 (see Annex C), EDP shows that risk management is a key pillar of its global strategy, ensuring that the group faces "controlled risk" levels in its business. For this purpose a number of policy decisions, actions and metrics have been defined that "ensure low level of intrinsic risk" (EDP Energias de Portugal, 2012, p. 117) for the group, despite the complexity of its business, its geographical coverage and ownership structure. The remaining two of the pillars upon which the strategic priorities are defined include 'superior efficiency' and 'focused growth'. This is similar to how Lufthansa depicts its corporate governance approach, having risk management as one of their three pillars.

Elements of the risk management process include, among others:

- A risk identification and assessment step, revolving around the aforementioned risk register, ensuring that "this process is included in the usual cycle of preparing the business plan and budget, at least for the most important risks and from the point of view of top management" (EDP Energias de Portugal, 2012, p. 117).
- Risk owner identification, allocating and delegating responsibilities to individuals in charge of mitigating the occurrence and/or impact of identified risks.
- Risk appetite, "considering [...] the way in which the group plans to grow [...], how it is going to obtain funding for this [...] and what rating it wishes to maintain or obtain, by endeavouring to satisfy appropriate ratios. [...] From a strategic perspective, the group defines the overall limits on its activity – vision – and its commitments in its Annual Report and Accounts."

The publicly available Risk Management Policy (on EDP's website) communicates the upper managements' position on risk and involves all employees. It gathers all involved around the main objective of minimising exposures, considering all risks from a portfolio perspective and stressing the importance of having an integrated approach to risk

management within the group, respecting local policies and legal requirements wherever the group operates.

Figure 94: EDP Energias de Portugal Corporate Business Risk Management Policy

edp > About EDP > Principles and Policies > Corporate Business Risk Management Policy

Corporate Business Risk Management Policy

Business risk management, which involves identifying, measuring, dealing with and reporting the main risks, is an integral part of the management style that the Group requires from its employees, in line with good international risk governance practices, legal and regulatory requirements and the Group's internal and external stakeholders' expectations and demands.

The Group's corporate business risk managment policy is based on the following principles:

> Risk management is everyone's responsibility, from the EBD to each individual employee. Everyone is responsible for knowing the risks in their area of activity and managing them in accordance with approved risk policies and tolerance levels.

> The Group must manage its significant risks from a portfolio perspective, optimising the balance between risk and return throughout all its business areas.

> Business risk management must be included in all the most important business processes, such as strategic and business planning, operations management and investment decisions, in order to ensure that risk analysis is included in all decisions.

> Business risk management is a comprehensive, continuous, disciplined process in which risks are identified, analysed and consciously accepted, increased or mitigated within approved risk tolerance levels.

> Local risk management polices and procedures must be consistent with this corporate policy. In addition, all local policies and procedures must facilitate the aggregation, consolidation and revision of all significant risks at corporate level.

Source: (EDP Energias de Portugal, 2013a)

The Annual Report also shows a description of the most important activities conducted involving risk management. Based thereon it is possible to see that:

- EDP engages in industry cooperation and communication on risk-related issues: “Active contribution to Eurelectric’s focus group Enterprise Risk Management, Task force Risk Analysis and Recommendations on Eurelectric’s Power choices Study and investment Action Plan” (EDP Energias de Portugal, 2012, p. 118). Eurelectric is the representative body of the European electricity industry listing as its mission “to contribute to the development and competitiveness of the electricity industry, to provide effective representation for the industry in public affairs and to promote the role of a low-carbon electricity mix in the advancement of society” (EURELECTRIC, 2014).
  This shows a complete opposite picture of the aviation industry, where individual airlines tend to avoid such discussions (as seen in the interview process) and industry bodies seem not to favour such exchanges. When contacted, the Association of European Airlines dismissed any further information sharing as “the AEA is not active in areas which are commercially sensitive for its members and,

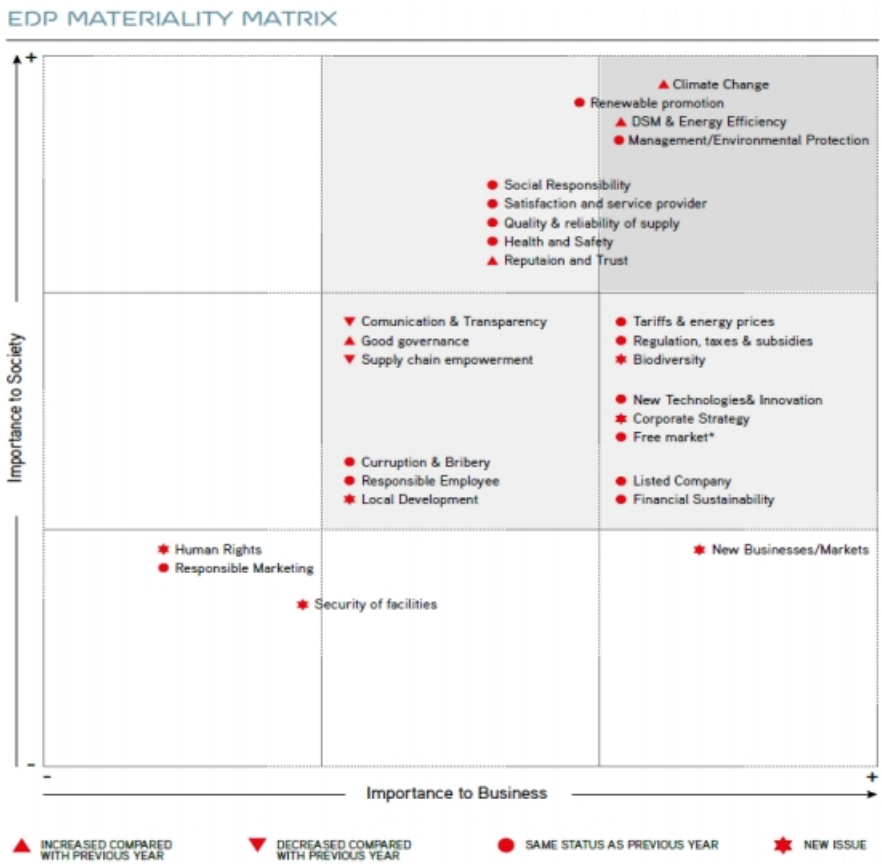
therefore, we do not have a risk management specialist on our team." As seen before, also IATA's working group on risk management does not seem very active.

- EDP conducts a bottom-up risk management exercise in parallel to a top-down analysis, all complemented by a benchmarking exercise with competing companies and a macro-economic analysis to the group and every subsidiary in their respective legal, social and economic environment. "The aggregate bottom-up risk analysis models were reformulated to increase the accuracy of risk measurements and allow different behaviours and non-linear associations between the different businesses' main risk factors. [...] We conducted an aggregate top-down analysis of the risk and compared it with competing companies. It continued to show a low degree of aggregate risk for the EDP group's businesses. [...] We analysed the country risks of the countries in EDP's current portfolio and those identified as targets – diversification effect and impact on the risk of the group's portfolio" (EDP Energias de Portugal, 2012, p. 118). This stresses the internal and external views on the company and all possible sources of risk. As seen, some airlines tend to have – or publicly report – only few of such activities.
- The group also performs risk analysis based on complex mathematical models, in order to help assessing the importance and impact of each risk on a number of criteria. This also shows that EDP is engaged with the scientific community in improving its evaluations methods. "Methods were developed for forecasting trends, volatilities and correlations of commodities and exchange rates followed by publication of a scientific article, internal use of the bottom-up risk analysis model and a quarterly report" (EDP Energias de Portugal, 2012, p. 118). Unlike most airlines, this company performs extensive Monte Carlo analysis and Value-at-Risk modelling, having some of its key performance metrics linked to such results as Return-at-Risk on Assets and on Equity, for example, comparing these to selected peers and competitors.

EDP's risk management process also enables capturing positive risk elements. For example, the recent acquisition of a large shareholding position by China Three Gorges enabled EDP, as per own statement, to get "access to the Chinese financing market. This was highly important in achieving the company's desired liquidity levels" (EDP Energias de Portugal, 2012, p. 119).

As part of the Global Reporting Initiative requirements, EDP publishes a Materiality Matrix where it consolidates (EDP Energias de Portugal, 2013d) elements that can have an importance on the business and on society. This is a way to engage with all stakeholders and address issues related to the companies' core business. A similar depiction has been presented by Cathay Pacific Airways as shown in the previous chapter.

Figure 95: EDP Energias de Portugal Materiality Matrix 2013



Source: (EDP Energias de Portugal, 2013d, p. 54)

EDP cites the COSO and COBIT reference models for its internal control and internal auditing framework, but does not mention any of these for its risk management activities.

6.3.2. Telecommunications: Portugal Telecom

The telecommunications industry is, in some respect, very similar to air transport. It is a mass market high-tech industry that is very fragmented, highly competitive and with very low yields. There is a constant search for innovation to enable growth in a saturated market and for differentiation of own products and services from competition. Portugal Telecom (from now on PT) is at the heart of this, as it is considered to be one of the most innovative players in the market. It operates in a variety of geographical markets, was object of a hostile takeover that it successfully fend off, is undergoing an industrial cooperation alliance with Oi (the largest Brazilian operator) and plans to fully merge with Oi in 2014.

This shows the intense environment the company is operating in and why it must have a solid approach to risk management. PT was kind enough to open its doors to shed light onto its risk management function, providing information on how the company is organising this function at a corporate level.

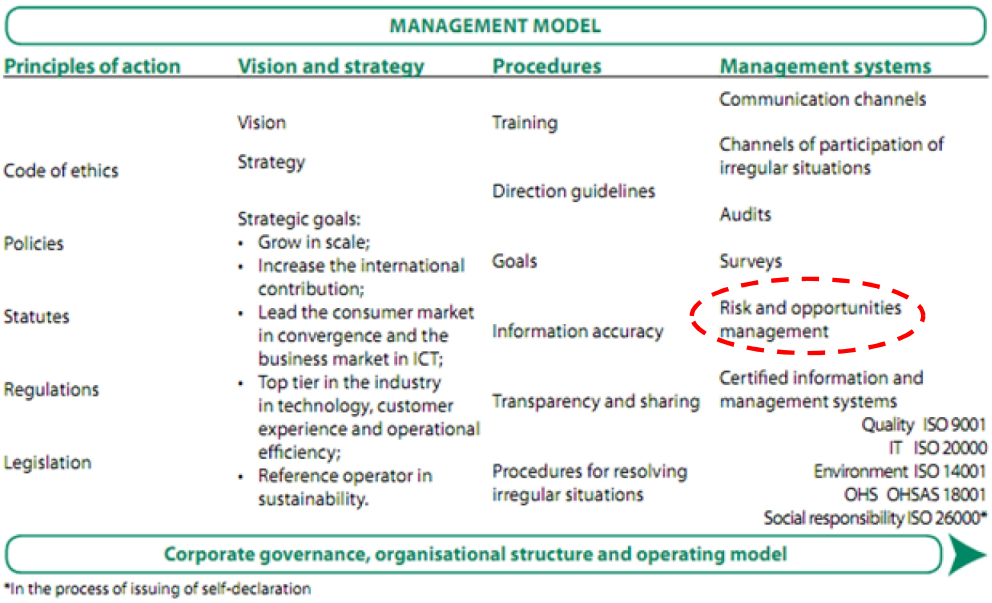
PT stated that it is following the COSO guidelines for internal control and risk management, mainly because it is listed at the New York Stock Exchange, therefore being forced to comply with SEC risk management requirements. As per PT's statements, COSO is commonly used in North America for risk management models, thus it was easier for PT to adopt it not only for US-compliance purposes, but corporate-wide implementation.[23]

While being integrated with Internal Audit, the risk management functions report hierarchically to the CEO and CFO and functionally to the Audit Committee. Periodic reviews are carried out, not only to assess new and current risk items, but also to evaluate the effectiveness of the entire risk management approach.

"As a structured and systematised approach, risk management is integrated in the company's strategic planning and operational management procedures, and relies on the commitment of all employees to adopt risk management as an integral part of their duties, notably by identifying, reporting and implementing risk mitigation measures and behaviours" (Portugal Telecom, 2013a, p. 51). Risk management is therefore integrated into the whole governance model and is thus an essential management system along with the remaining communications, quality and auditing functions, helping the organisation achieving its strategic goals (see Figure 96: Portugal Telecom Management Model).

[23] As seen in the previous chapter, the survey to the Annual Reports of the top 100 airlines revealed that most US-based airlines also follow COSO guidelines.

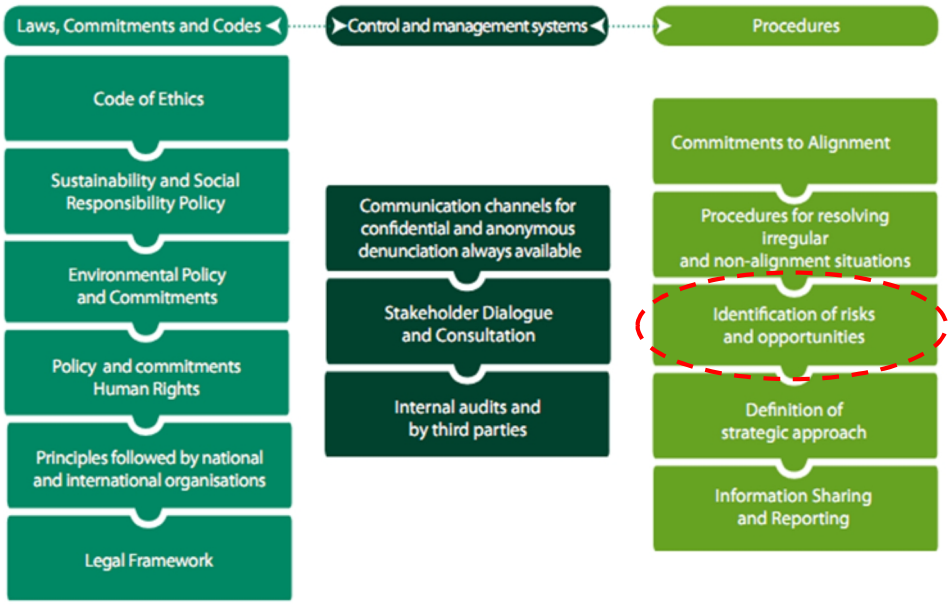
Figure 96: Portugal Telecom Management Model



Source: (Portugal Telecom, 2013c, p. 37), own highlight

This is further detailed by explaining how PT involves risk management in the triple bottom line process areas: ethics, environment and society. Stakeholder dialogue is at the centre of this process, as part of fundamental control and management systems. How PT relates to and involves stakeholders in its management processes will be further detailed below. This is probably the most valuable contribution of PT's risk management process.

Figure 97: Portugal Telecom transparency and compliance in the value chain



Source: (Portugal Telecom, 2013c, p. 47), own highlight

The Corporate Governance Report lists a long list of goals that PT's risk management function is intended to pursue. They include:

- "Implementation of a corporate risk management model in line with the PT Group's strategic goals;
- Identification and analysis of the main risks to which PT and its subsidiaries are exposed within the framework of the conduct and pursuance of their business;
- Identification and analysis of the main risk factors and events that may significantly affect operation in the normal course of PT and its subsidiaries in terms of:
    - Impact;
    - Probability of occurrence;
    - Associated control level and response capacity in a crisis;
    - Speed at which the risk or event may materialise;
    - Identification of improvements in control and follow-up of mitigation plans associated to critical risk factors;
- Improve the quality of information supporting the decision-making procedure;
- Communication of the results of the risk management process and warnings in the event of occurrence or identification of new critical risks" (Portugal Telecom, 2013a, p. 52).

Relevant here is to stress that PT does not limit the risk analysis to the traditional two-dimensional impact and probability analysis, but expands this to at least three other elements: control level, speed of materialisation and improvements in controls. This could be an interesting add-on for an airline risk management framework.

Two essential elements to PT's risk management approach are a 'risk dictionary' and their own 'risk management methodology'. The risk dictionary lists a variety of possible risks and their allocation to three main categories relevant for PT's business:

- "Strategic Risks: These correspond to risks that depend on external factors to the PT Group that might affect its performance, strategy, operations and organisation. Due to their nature, the origins of environment risks imply that their associated impact must be appropriately anticipated and the materialisation of their associated risk factors and mitigation strategy in the event of a crisis must be timely identified.
- Operational Risks: These result from and are inherent to business activities and internal processes, and management may ensure their control at their origin, in a preventive manner.
- Financial Risks: Associated to the PT Group's financial performance and to the transparency in its communication to the market." (Portugal Telecom, 2013a, p. 53)

The risk methodology establishes responsibilities for risk identification, evaluation, management, monitoring and process review. Clear tasks are distributed and shown.

Figure 98: Portugal Telecom Risk Management Methodology

Risk Management Methodology	
Executive Committee	Identify main risks affecting PT Group Define Risk Managers Decide on action & prioritisation of mitigation actions
Audit Committee	Evaluate risk management model Propose improvements & changes to model Review the main risks
Risk Management Function	Support the definition & implementation of a risk management model in line with best practices Monitor risk management model & ensures that the information from different PT Group companies is correctly integrated Support Executive Committee & Audit Committee in defining materially relevant risks Follow up action plans required to guarantee correct treatment of identified risks
Business Management Risk Managers	Manage materially relevant risks Implement actions required to ensure appropriate control Evaluate & quantify residual risk to which the company is exposed Identify critical areas of risk exposure and propose mitigation actions Re-feed Risk Management Model, and warn about exposure situations or control environment degradation
Internal Audit Function	Evaluate the effectiveness of control mechanisms at reliability & integrity level of financial & operational reports, efficiency of operations & compliance with laws & regulations.

Source: (Portugal Telecom, 2013a, p. 54)

The interaction of these five entities is depicted as a circular process, where the integrated methodology is approved separately and informed by the Executive and Audit Committees to the risk management functions (risk teams and risk managers) in all subsidiaries and business units. Their task is to conduct the risk management process in a manner effective with the pre-established goals, assessing PT's exposure to identified risks. This is then consolidated and escalated to upper management for review, response and monitoring.

This Annual Report shows that PT's risk register contains 312 risk factors, which are then filtered, summarised and consolidated by the corporate risk management function into – as per interview statements – six core risk factors that are escalated to upper management.

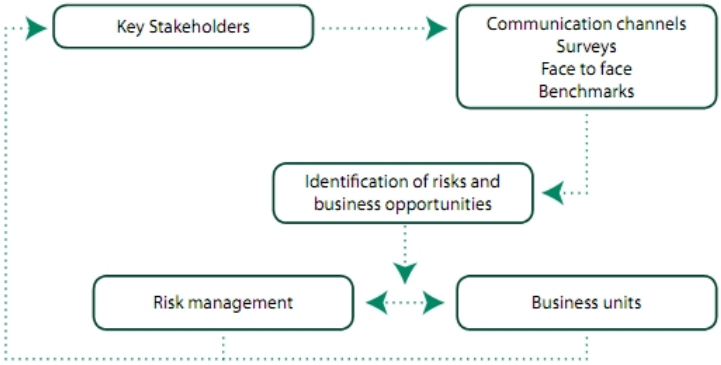
What also strikes in PT's risk management approach is their involvement of stakeholders, whose interests are analysed by a variety of sub-committees performing a cross-cutting analysis across the entire value chain. These areas include (Portugal Telecom, 2013c, p. 85):

1. "Energy and Environment;
2. Labour Relations, Human Rights, Occupational Health and Safety;
3. Stakeholder and Supplier Relations;
4. Communication, Branding and marketing of Products and Services;
5. Innovation and Development of Services and Solutions;
6. Citizenship and Personal Responsibility;
7. Sharing of Sustainability Practices with International Subsidiaries."

Figure 99: Portugal Telecom Stakeholder Relationship Model

Source: (Portugal Telecom, 2013c, p. 70), own highlight

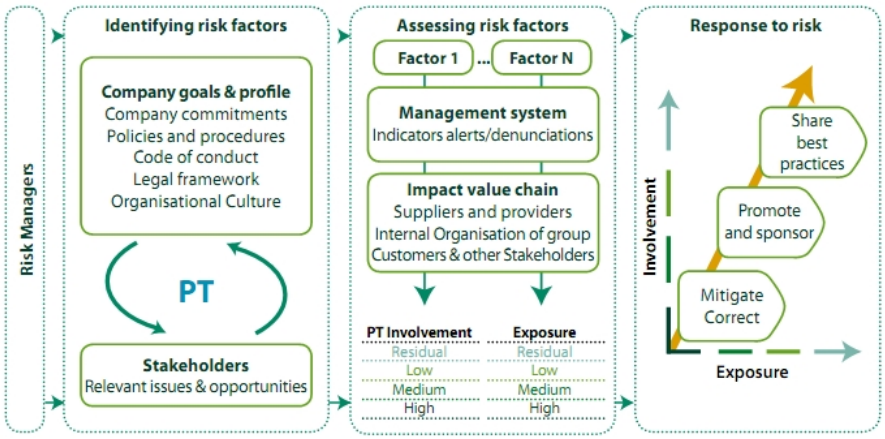
Figure 100: Portugal Telecom Strategic Consultation Model



Source: (Portugal Telecom, 2013c, p. 71)

The strategic consultation process enables key stakeholders in participating in the information and knowledge exchange, allowing risks and opportunities to be properly identified and treated within all business units. This is also described in the sustainability committee where stakeholders actively engage in identifying relevant issues and opportunities. PT then takes this input through the methodological steps of the risk management process in order to prepare a proper risk response plan.

Figure 101: Portugal Telecom Sustainability Committee



Source: (Portugal Telecom, 2013c, p. 86)

6.3.3. Other industries: surveys from Management Consultants

The above two cases represent just two of all possible industries. Visiting representative cases of all remaining ones would not only be impractical, due to time and resource restrictions, but also redundant as there are plenty of published surveys on risk management practices covering a variety of industries. Some have already been mentioned in previous chapters, whenever their content was relevant for the topic under discussion. This section will focus on their main findings, highlighting the specific elements from individual industries, in an attempt to filter more lessons for the core goal of this thesis: design an aviation specific application framework of the ISO 31000 risk management standard.

As the generic topic of risk management has gained visibility and importance over the years, more surveys have been published not only by large management consulting firms, insurance companies and brokers, but also industry associations and risk management forums. A non-exhaustive list of these includes:

- *European Risk Management Benchmarking Survey 2012* published in October 2012 by the Federation of European Risk Management Associations (FERMA, 2012);
- *Special Report: Excellence in Risk Management, Delivering Strategic Value Through Risk Management* published in April 2013 by Marsh (a global risk management consulting and insurance firm) and the Risk Management Society (a global non-profit organisation dedicated to improving risk practice) (Marsh, 2013);
- *Insight Report: Global Risks 2013, Eighth Edition*, published in January 2013 by the World Economic Forum (World Economic Forum, 2013a);
- *The Global Risk Management Survey 2013*, published by AON Risk Solutions, another risk management solutions provider in the fields of insurance, reinsurance, brokerage and advisory services (AON, 2013);
- *Expectations of Risk Management Outpacing Capabilities – it's time for action*, a special report on risk management by KPMG one of the largest global consulting firms; this includes results of a survey conducted by the Economist Intelligence Unit (sponsored by KPMG) to over 1000 C-level executives from, mainly, five "industry clusters": financial services; technology, media & telecommunications; diversified industrials; healthcare; and energy & natural resources (KPMG, 2013);
- *The Accenture 2013 Global Risk Management Study - Risk management for an era of greater uncertainty*, containing a quantitative survey to over 440 organisations from seven industries (insurance, banking, energy, utilities, healthcare, capital markets, life sciences, government administration, postal) conducted by Accenture and Oxford Economics (Accenture, 2013);
- *The Deloitte Global Risk Management Survey, Eighth Edition,* by Deloitte, another consulting firm, focussing on the financial services sector (Deloitte, 2013);

- The Ernst&Young report on *Turning Risks and Opportunities into Results - The top 10 risks and opportunities in the light of the current economic environment*, published in March 2012 (Ernst & Young, 2013);
- The Harvard Business Review paper on *Leadership in Risk Management*, including survey results to 217 C-level executives of mostly European companies (Harvard Business Review, 2013);
- And the aforementioned, slightly older, *Global ISO 31000 survey 2011*, conducted for the ISO 31000 Conference by the G31000 Global Risk Management Platform (G31000 Global Risk Management Platform, 2012) covering 1823 participants from 111 countries and 28 industries.

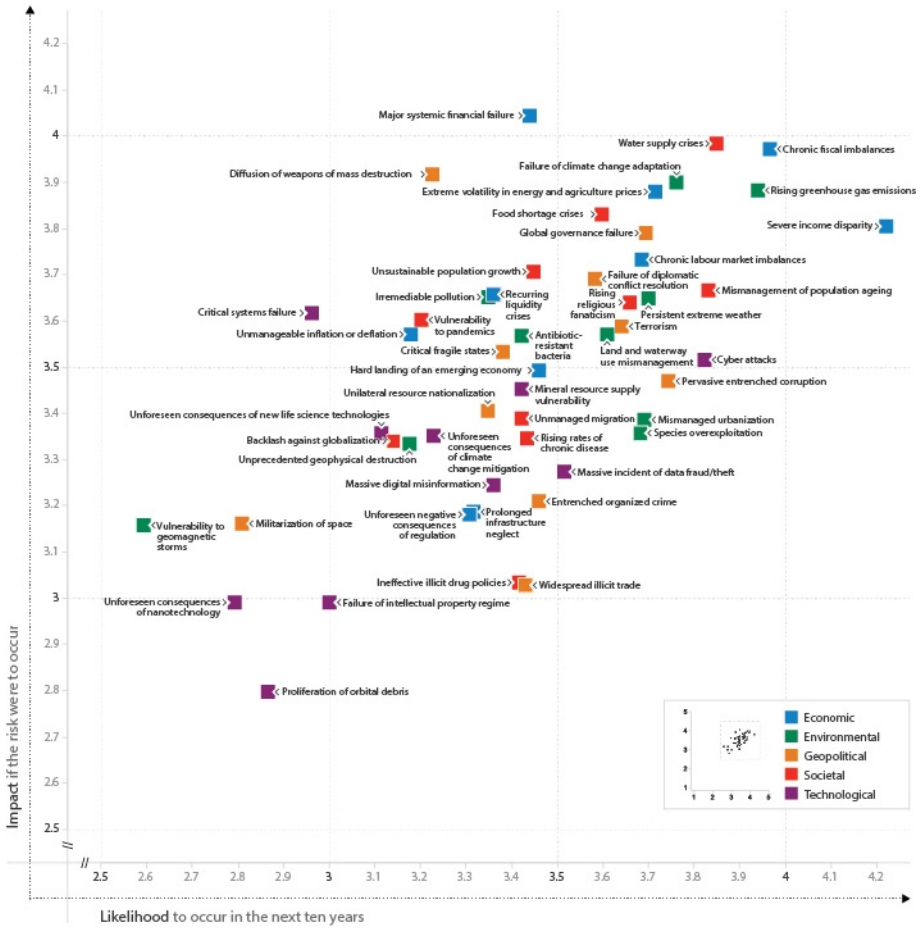
Many more articles and reports exist covering similar surveys and topics from other large organisations, some of them have also been mentioned in previous chapters. It is not intended to reproduce all of these reports in this section, but to summarise and filter the most interesting findings for the case at hand.

All of these surveys present a list of key risks as identified by participants. The report by the World Economic Forum (WEF) shows not only the full risk landscape (split between economic, environmental, geopolitical, societal and technological risks), but also how interconnected individual risks are among themselves (World Economic Forum, 2013a). Both enable interesting conclusions.

While the large risk landscape is not made specific for any particular industry (see Figure 102: WEF Global Risk Landscape 2013), every single entity - regardless of its industry - should be asking itself how its risk model captures these risks (if at all), how these risks can affect its own business and how prepared the organisation is to face these risks. Even if the risks contained in this report tend to be macro-risks, of political, social, economic or other natures, one should not neglect reviewing their impact on, for example, the airline industry as it is highly interconnected and exposed to external shocks. Understanding the world where the specific company operates in will help it better integrate and face risks. Risk management must, by definition, be a broad and overwhelming exercise.

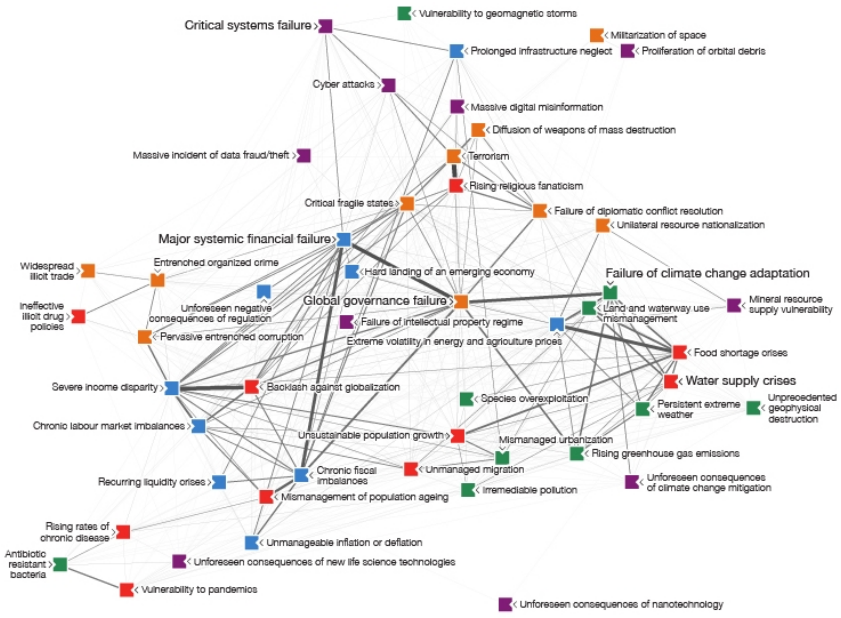
The interconnections between individual risks (see Figure 103: WEF Risk Interconnection Map 2013) enables entities to understand the gravities in their risk landscape: what elements are influencing each other, how does solving the “heaviest” risk help mitigating and reducing the impact or likelihood of a number of other risks that depend on this one. Visually this results in a dense cobweb with lines showing the interconnections among all individual risk items.

Figure 102: WEF Global Risk Landscape 2013



Source: (World Economic Forum, 2013a, p. 5)

Figure 103: WEF Risk Interconnection Map 2013



Source: (World Economic Forum, 2013b, p. 53)

The AON Global Risk Management survey lists risk landscapes and top risks down on industry level. 'Economic slowdown / slow recovery' is the most important risk for the majority of the industries surveyed, including aviation. For this in particular 'increasing competition' and 'failure to innovate / meet customer needs" are listed in second and third place respectively (AON, 2013, p. 43). Moreover the survey goes into risks arising over "the next three years", showing that some movements in risk ranking are expected.

Figure 104: AON Global Risk Management Survey – Snapshot of Top Risks by Industry

Top three risks by industry

Industry	Key Risk 1	Key Risk 2	Key Risk 3
Agribusiness	Commodity price risk	Weather / natural disasters	Regulatory / legislative changes
Aviation	Economic slowdown / slow recovery	Increasing competition	Failure to innovate / meet customer needs
Banks	Regulatory / legislative changes	Economic slowdown / slow recovery	Damage to reputation / brand
Chemicals	Economic slowdown / slow recovery	Commodity price risk	Exchange rate fluctuation
Conglomerate	Economic slowdown / slow recovery	Increasing competition	Exchange rate fluctuation

Source: (AON, 2013, p. 43), own highlight

The question here is to understand how these industries identify risks and organize risk management activities. The report provides only an aggregated picture, not by industry, but from a regional perspective. It is possible to see (Figure 105: AON Global Risk Management Survey – Risk identification) that roughly a third of all participants suggest risk identification should be done by a 'structured enterprise risk identification process', but that many more rely on 'senior management experience' to do so (AON, 2013, p. 63). Unsurprisingly – and in line with conclusions taken in previous chapters – the Asia-Pacific region is where a 'structured enterprise risk identification process' gathers most support.

Figure 105: AON Global Risk Management Survey – Risk identification

Identification by region

Category	All	Asia Pacific	Europe	Latin America	Middle East & Africa	North America
Board and / or management discussion of risk during annual planning, risk assessment or other processes	60%	66%	58%	52%	69%	61%
Senior management judgment and experience	58%	65%	48%	50%	55%	70%
Risk information from other function-led processes (e.g. internal audit, disclosure, compliance, etc.)	45%	54%	31%	52%	55%	53%
Industry analysis, external reports	30%	32%	21%	31%	38%	38%
Structured enterprise wide risk identification process	33%	43%	29%	31%	31%	34%
Other	2%	1%	2%	3%	10%	2%

Source: (AON, 2013, p. 63)

As for risk assessment, the picture is not very different: just 26% of all participants suggest this is part of a structured enterprise-wide process, with Asia-Pacific being the region where this is most supported. North America relies most on senior management judgement and experience.

Figure 106: AON Global Risk Management Survey – Risk assessment

Assessment by region

Category	All	Asia Pacific	Europe	Latin America	Middle East & Africa	North America
Board and / or management discussion of risk during annual planning, risk assessment or other processes	46%	51%	42%	49%	52%	46%
Senior management judgment and experience	62%	64%	53%	54%	55%	73%
Risk Modeling / risk quantification analysis	34%	33%	33%	32%	45%	36%
Consult with external service provider/advisor	29%	31%	19%	44%	31%	35%
Structured enterprise-wide risk identification assessment process supported by a standard toolkit and methodology	26%	42%	20%	28%	28%	25%
Other	2%	0%	2%	2%	3%	2%

Source: (AON, 2013, p. 66)

From an organisational point of view, a large percentage reject having or planning to create a Chief Risk Officer position, although this is supported by most risk management standards addressed in previous chapters. It would be expectable to see this decreasing over time, but the opposite tendency is visible: this percentage increased over the years, which is inconsistent with other messages stressing more importance and visibility given to risk management within the organisations. The authors suggest “The existence or absence of a CRO appears to be correlated with a company’s size. Seventy-eight percent of organisations with revenues less than USD 1 billion indicate that they do not have a CRO, as opposed to 56 percent for organisations with more than USD 1 billion in revenue. From an industry standpoint, highly regulated sectors such as banking, utilities, insurance, investment and finance are more likely to have an established CRO position” (AON, 2013, p. 83).

Figure 107: AON Global Risk Management Survey – Role of the CRO

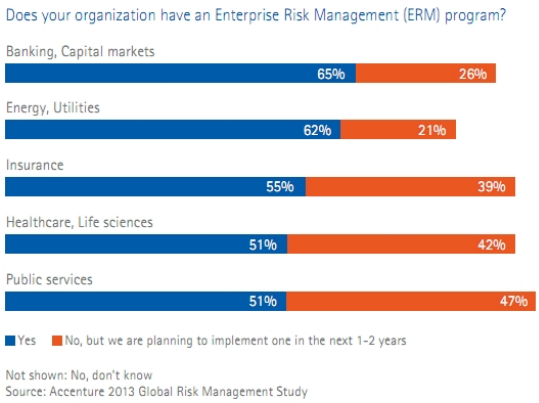
Role of the CRO

Role	2013	2011	2009	2007
Yes, but this role does not include risk management	10%	12%	11%	8%
Yes, this role includes risk management	18%	19%	14%	17%
No, but we are considering creating this position	7%	6%	10%	10%
No, and we do not plan to create such a position	63%	60%	62%	60%
Don't know	2%	2%	3%	4%

Source: (AON, 2013, p. 83)

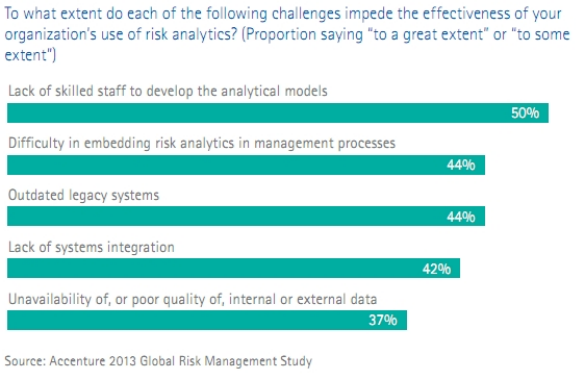
The survey produced by Accenture indicates that 96% of participants say their companies have the CRO position, while in 2011 this was just 78%. From an industry perspective the majority says they have an Entreprise Risk Management Program, with many of the remaining suggesting that they are planning to implement one over the next years. Banking and Capital Markets stand out as 65% of these companies have an ERM-program, while just 51% of Public Services refer to the existence of such a program in their organisations (Accenture, 2013, pp. 21-22).

Figure 108: Accenture Risk Study: Adoption of ERM by Sector



Source: (Accenture, 2013, p. 22)

Figure 109: Accenture Risk Study: Obstacles to effective risk analysis

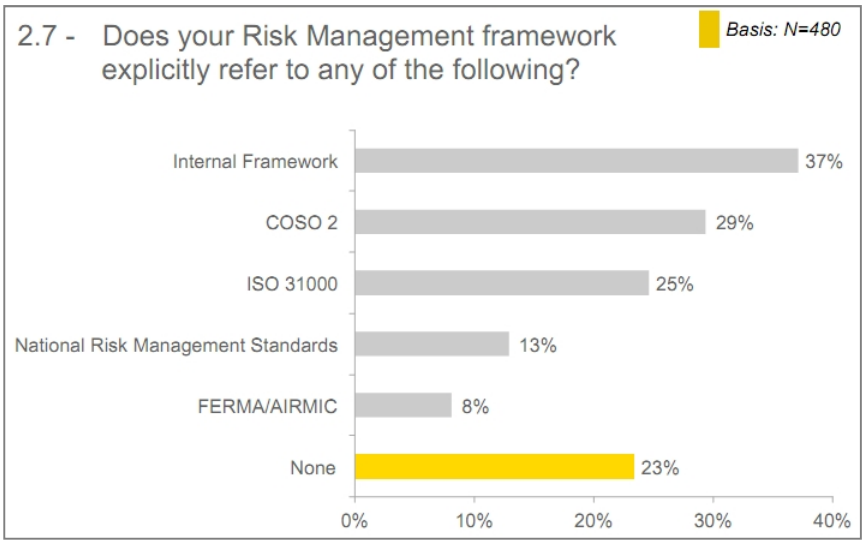


Source: (Accenture, 2013, p. 30)

In terms of challenges to effective risk analysis, the participants select the lack of skilled staff as the most important reason, collecting 50% of preferences, but closely followed by 'difficulty in embedding risk analytics in management processes' and 'outdated legacy systems' both with 44%. There is no industry-breakdown for this question. It therefore seems that staff training and development is key to improving risk analysis within organisations (Accenture, 2013, p. 30).

This is also one of the key findings of the FERMA Benchmarking Survey, where 57,6% of all participants state that they don't have any specific qualification in risk management. Just 16,9% refer to University Degree and about 5,8% to executive training provided by the Institute of Risk Management (FERMA, 2012, p. 71). This survey explicitly asks participants on risk management standards applied by their organisations. Out of all, 37% refer to the use of an Internal Framework, followed by COSO for 29% and 25% choosing ISO 31000 (FERMA, 2012, p. 80).

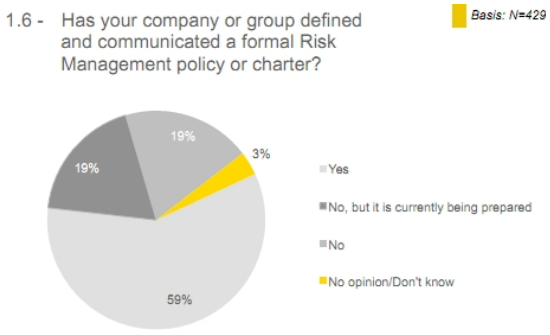
Figure 110: FERMA Survey – Use of specific standards



Source: (FERMA, 2012, p. 80)

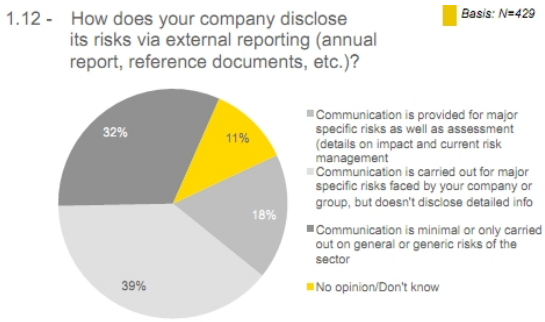
In terms of internal and external communication, 59% of the survey participants suggest their companies have a formalized risk management policy, although 39% say that external communication focuses on major risks only, without disclosing critical details. Just 18% admit a more detailed reporting of risks faced by their organisation (FERMA, 2012, p. 76).

Figure 111: FERMA Benchmarking Survey – existence of a Risk Management policy



Source: (FERMA, 2012, p. 75)

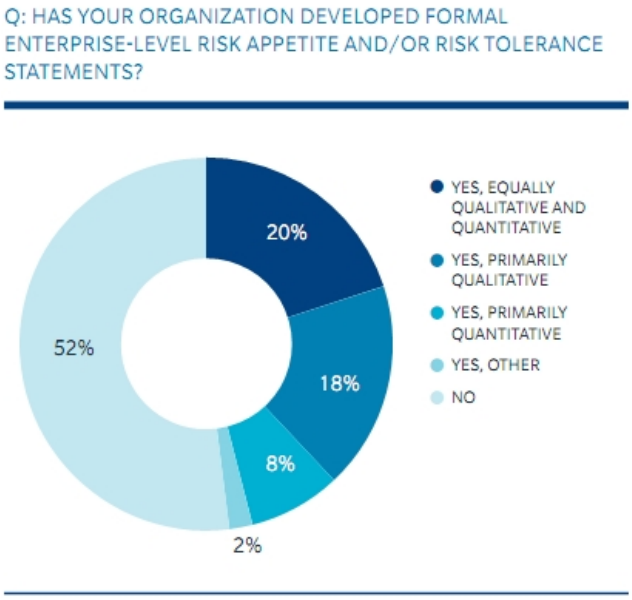
Figure 112: FERMA Benchmarking Survey – risk disclosure and communication



Source: (FERMA, 2012, p. 76)

The Marsh Survey for RIMS comes to a different conclusion: 52% of the respondents decline having a formal risk appetite and/or risk tolerance statements, and based on this suggests that organisations should “develop formal enterprise-level risk appetite statements” to help stakeholders better understand and assess the capacity to retain risk given the financial strength and performance of the organisation” (Marsh, 2013, p. 17).

Figure 113: Marsh Survey – Risk Appetite and Risk Tolerance Statements



Source: (Marsh, 2013, p. 7)

Other recommendations by Marsh include:

- "Establish key risk indicators (KRIs) that will guide the overall risk framework within your organisation";
- "Help to increase education at the board level around enterprise risk management, strategic risk management, and related techniques used to identify and assess risk and to report the results across the organisation. This can help to build strong sponsorship and commitment to risk management at senior levels of the organisation."
- "Use data analysis and aligned tests to support the organisation's overall risk strategy as a means to close the gap between being a cost center and a strategic thought center."
- "Build a more relevant central risk function, as some have already put in place that will coordinate risk discussions across the entity and identify, assess, and strategize cross-organisational risk solutions."
- "Develop performance measurements to more clearly demonstrate the value that risk professionals bring, beyond insurance and claims cost reductions." (Marsh, 2013, p. 17)

Suggestions like these shall be considered for adapting the ISO 31000 framework to the airline context. The next section will outline the key improvement potentials identified for that adaptation, while also taking into consideration all lessons learned from other industries.

6.4. Chapter summary: identified elements for improvement

Given all findings from the discussion conducted above it is now possible to identify key elements for improvement upon which this thesis is designing its major proposal. As already mentioned, more than proposing a radical new risk management standard, this thesis is going to propose an adaptation of the ISO 31000 framework to the airline environment. ISO 31000 considers risk in its holistic existence, thus covering the positive and negative aspects; more than COSO or other standards that have partial views only. Moreover, it has already been shown that ISO 31000 can be used as risk management standard within the airline industry, as some airlines already do, although these are still a minority. This thesis will keep the ISO 31000 risk management process as it has proven to be effective. By proposing an adaptation just of the ISO 31000 framework, it is expected that airlines find the ISO 31000 process easier and friendlier to use, more than other available standards. Therefore, following key requirements can be listed for such an adaptation to be attractive:

- An adapted framework must be simple and easy to understand to allow for an intuitive implementation by airlines. Risk management should cover more than immediate and visible risk factors and enable discussions on fundamental issues.
- It must be holistic and integrating, covering not only operational issues already naturally handled in airline operations, but also all business issues related to the airlines' management from a corporate perspective.
- It is therefore essential that risk management becomes aligned and integrated with the airlines' strategic planning processes.
- It should enable the involvement of all stakeholders, internal and external, capturing their opinions on the companies' operation and critical issues.
- It should also equip upper management with tools to help taking better, more informed and quicker decisions, as means to improve resilience and thus reduce risk in daily operations and management while identifying and exploiting potential opportunities that arise from the process.
- As key management process, the risk management process should become part of the airlines' value chain, having all required resources and management visibility as a stand-alone unit within the company.
- From an organisational perspective such a risk management unit should be independent from Internal Audit, as these functions are not directly linked with each other: Internal Audit should also be able to assess the validity and efficiency of the risk management process; something it cannot do if it is integrated.

Based on this, the next chapter will outline all characteristics of the proposed framework adaptation. This will then be object of validation as explained in the subsequent chapter.

7. Proposal for adaptation of the ISO 31000 framework to the airline industry

Air transport is probably one of the most regulated, fragmented, competitive, volatile and least profitable industries. It is technology and capital intensive, object of political interference, highly dependent on the local, regional and global economic prospects, but suffers from chronic infrastructure restrictions on the ground, in the air and supply chain disruptions. It has been used as prestige object by politicians and also as political weapon against civilians. Plenty of literature has been produced to describe the airline business (e.g. (Clark, 2010), (Belobaba, et al., 2009), (Doganis, 2002) and many others), and all highlight the same critical topics. These characteristics occur simultaneously, but it is still a business, probably like any other, that has natural challenges to be dealt with and opportunities to be grasped.

Risks can arise from a variety of sources and can be classified according to: their origin – internal or external; and their type – strategic, financial, operational and hazard. When there is little management capability and oversight, or limited resources, their impact can have devastating effects. Previous sections have shown typical airline risk factors (see Figure 59: Airline Risk Factors) and a sample airline value chain (see Figure 84: Typical airline value chain), with all key functions of an airline. It has been shown that risk management is traditionally not part of that value chain, although it should be present throughout the entire organisation. Proper risk identification, management and mitigation strategies – as proposed by plenty generic risk management standards – can help companies overcome challenging situations.

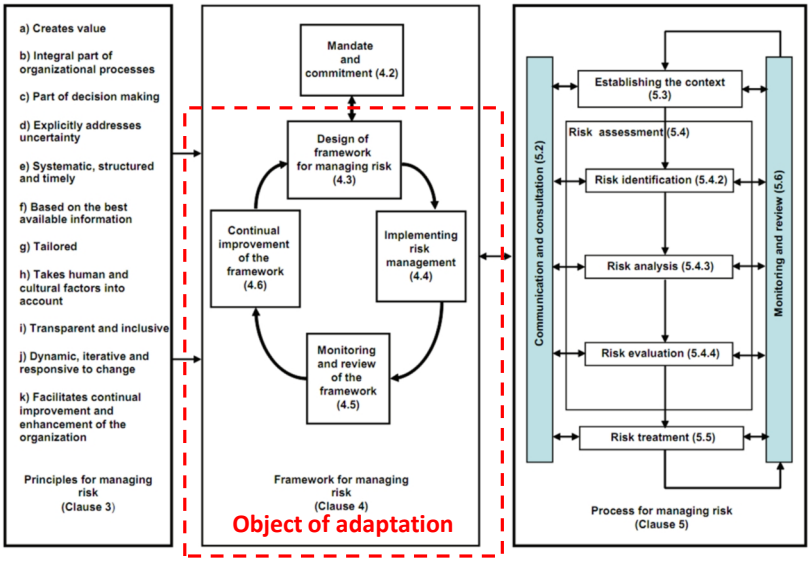
And yet, airline-specific risk management standards are either only focused on safety and operational issues (ICAO) or ignored by the airline community (IATA) and industry-neutral standards are in most cases not completely applied, leaving a minority group of airlines that consistently apply risk management practices to the airline as a whole (and not as just a flying operation). Of all these, ISO 31000 has been chosen for adaptation to the industry.

Now that the key requirements for a framework adaptation have been set, based on the conclusions drawn from the research conducted and the lessons learned from other industries analysed in the previous chapters, it is necessary to outline a proposal for that adaptation. The following sections will list the overall goals such an adapted framework must achieve, provide a broad overview of the key elements, as well as detail step-by-step descriptions of the individual components of the proposal.

7.1. Goals and vision

As exposed in previous sections, the ISO 31000 standard is based on a set of principles, a framework and a process for managing risk. The principles are clear and the base for the whole approach. The process is also simple and easy to understand. It is the framework linking principles to process that causes some friction when it comes to the actual implementation. This framework revolves around five steps that initiate with a 'mandate and commitment' given by upper management to a designated risk management team, who is then in charge of proposing a 'design of framework for managing risk', and then 'implement risk management', proceed to 'monitor and review' and the 'continual improvement of the framework'. This is a revolving process, but is still vague and industry-neutral, requiring some effort for adaptation to each industry and company. It is this framework that is proposed to be adapted to the airline industry, in order to facilitate its dissemination and implementation.

Figure 114: ISO 31000 framework as object for adaptation



Source: adapted from (International Organisation for Standardisation, 2009a)

Major goal of this adaptation will naturally be to help airlines reduce risk in their daily operation and management. Such an adaptation must therefore cover operational areas, as well as key strategic management areas, that under the traditional industry-specific approaches are left aside. This adaptation must also enclose the internal and external elements of the airline, regarding its organisational set-up or its surrounding environment, in order to capture potential risks that may arise in these areas. This stresses the holistic approach that is intended to be given to this proposal.

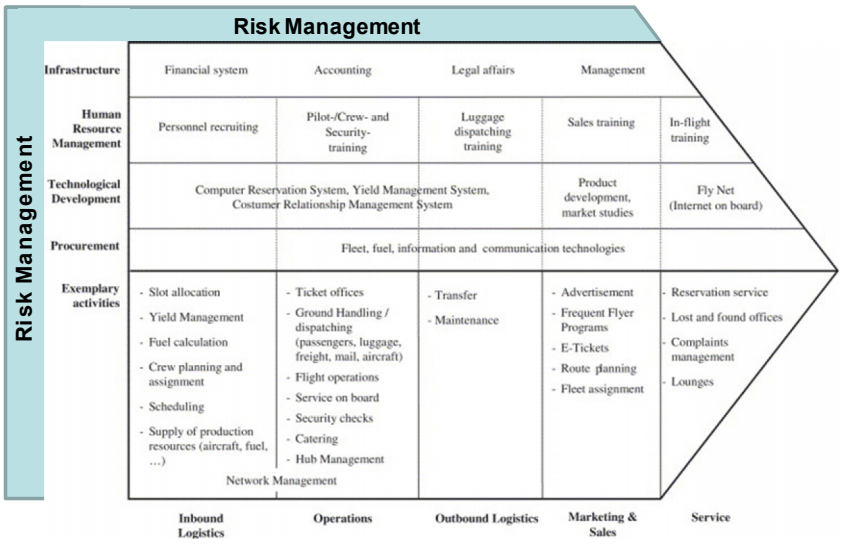
Therefore, this adaptation must help airlines introduce risk management practices to:

- Identify, assess and manage all risks (or as many as possible), without focussing on one area in particular;
- Focus on internal and external risks in their environment, but also involve their stakeholders in the risk management process;
- Help airlines achieve goals and create better management practices;
- Improve resilience to face a tough, changing and challenging business and operating environment.

This can only be achieved if the proposed adaptation is easily understandable; based on international best practice; industry-specific, yet still customizable by each airline; and adjustable to the needs and requirements of each airline.

If properly implemented, this should transform the typical airline value chain, where risk management is not present, into one where it is an essential part of the entire organisation and at the core of each individual function. In a recent interview to the Strategic Risk Magazine, Mr. Gordon Song (Head of Entreprise Risk Management and Internal Audit at Tigerair, a Singapore-based low cost airline), stated that "People still see risk management as a kind of a compliance-driven regime. I don't see many companies formally embedding risk management into processes like business development, supply-chain management, and due diligence on corporate transactions such as joint ventures" (Jones, 2013). This stresses the need to include risk management into the value and the supply chains.

Figure 115: Risk management centred airline value chain



Source: adapted from (Albers, et al., 2005)

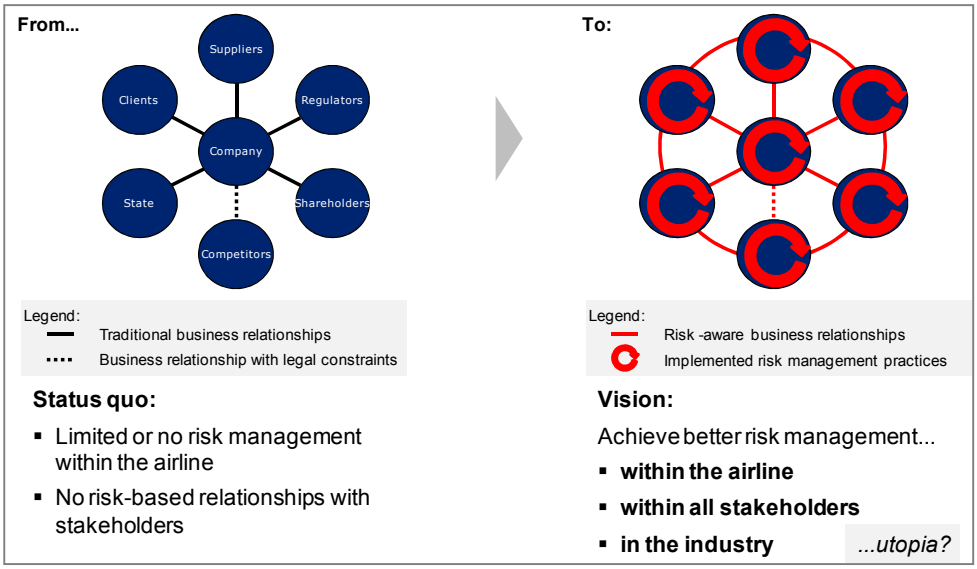
All these elements will serve as guideline for the proposal outlined in the section below.

The overall vision for this proposal is to make risk management not only a core element of the individual airlines' existence, ever present in upper as well as lower management levels across its entire value chain, but also to enable involving stakeholders in a joint risk management approach, thus reducing the risks that can occur in the airlines' surroundings, such as in its supply chain, shareholder panel, regulators, client base, state and – whenever possible[24] – competitors.

This involves transforming self-centred entities that relate to each other as clients, suppliers, shareholders, regulators or competitors, some without any attention given to risk or a harmonised process to manage risk, into an industry that is truly integrated and aligned around a common understanding of risk and the best way to manage it.

The current relationship models don't refer to risk, therefore individual organisations may or may not adopt a risk management standard of their choice. As seen before, each standard has diverging definitions of risk and approaches to manage it. If there is an internationally valid and recognized standard such as the ISO 31000, why not adapt and adopt that so that everyone speaks the same language?

Figure 116: Vision of an holistic risk management approach in the airline industry



Such a vision might be a utopia: something that will never be materialised due to technical difficulties, political opposition or legal hurdles. In any case it can be left as ultimate vision for further development.

[24] Antitrust laws may limit the extent to which airlines may cooperate on these levels.

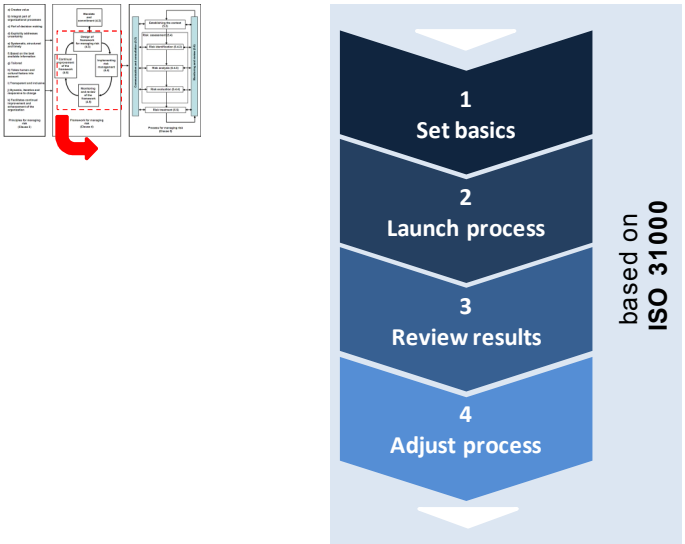
7.2. Design of the framework adaptation to the airline industry

Based on the goals and key requirements outlined above, the proposal for adapting the ISO 31000 risk management framework relies on four key features:

- Simplicity. One key criticism to other models is that they are too complex and heavy; “simplicity by design” should be at the forefront for easier understanding and acceptance.
- All-embracing. The airline business is already highly regulated and some areas (Flight Operations, Maintenance & Engineering) are very good in managing their own risks, yet there is rarely a common and uniform approach to all risks the airline is exposed to. This new framework should be able to accommodate all sorts of risks, regardless of their nature.
- Revolving. This is a dynamic industry impacted by all types of issues, from geo-political events to technological developments. Reviewing and adjusting the risk management results, processes, and responsibilities is essential.
- Based on ISO 31000. It is the latest, internationally recognized, industry-neutral and most intuitive standard. It contains a clear process description and harmonized language making it a good base for an airline specific framework

This set of features led to the design of a four-stepped framework that at first glance seems similar to the ISO 31000 framework, but distinguishes itself when the elements of the individual steps are disclosed and explained in more detail.

Figure 117: Adapted ISO 31000 framework to the airline industry – overview



This approach keeps the very first step ‘mandate and commitment’ as suggested by the ISO 31000 standard. It is still essential to set a clear mandate, with guidelines, leadership

responsibilities and tasks to a specific team that is going to own the risk management process. Subsequent steps include:

1. Set basics. Herein the goal is to understand the organisation and its activities in the specific industry, economic and social context (thus including internal and external issues), before launching the formal risk management process. There is no use for random action that is not targeted at specific needs of any organisation. This step includes elements of internal nature such as strategy identification, stakeholder identification, market identification and compliance level identification; as well as of external nature such as a value chain analysis and a supply chain analysis; accompanied by a global risk maturity definition of the airline and the respective risk appetite definition.
2. Launch process. Based on the ISO 31000 risk management process[25], airlines can increase the likelihood of achieving objectives by managing risks in a consistent and uniform manner. ISO 31000 is clear in its language and understandable in its process. Individual elements are: risk management process application; risk landscaping; risk organisation; risk evaluation and risk control identification.
3. Review results. Key questions to answer refer to the analysis of the process outcomes: Has any aspect been neglected? Is residual risk reduced to minimum significance? What shortcomings does the process still have? How can the process be improved? For this purpose, the organisation should conduct following individual exercises: goal measurement, process feedback, gap analysis, risk vs cost vs benefit analysis, risk sources vs effects analysis, and build a risk mitigation toolbox.
4. Adjust process. This step is all about implementing improvement potentials or change requests uncovered in the previous step. The whole framework can only live if it keeps its revolving and iterative nature, incorporating feedback collected from all involved counterparts. This is of a more qualitative nature aimed at reviewing with all functional areas the degrees of implementation and change required to adjust the whole process.

Due to its inherent revolving nature, the framework should keep revisiting these individual steps and incorporate changes if and where necessary. For example: changes in the internal or external context may impact the process depth or scope, thus requiring a new design of specific elements. This will then impact the results, or the criteria that are to be used in assessing the results achieved, therefore leading the further improvement potentials to be introduced in the whole exercise.

Details for each step and individual elements will be given in the next section.

[25] It should be stressed that 'risk management process' is still the one outlined by ISO 31000, including context establishment, risk identification, risk analysis, risk evaluation, risk treatment, all closely monitored and reviewed, with constant communication and consultation.

7.3. Description of individual proposal steps

This section will describe the steps and the respective elements of the adapted framework. These elements will allow capturing a good overview of the airline, in its commercial and strategic aspects, as well as highlighting the current understanding of risk within the organisation, before launching the actual risk management process. To start, as the title suggests, let's set the basics. The following sections will then elaborate on the process, results and adjustment steps of the proposal.

7.3.1. Set basics

After the organisation has set up a clear mandate for risk management, the respective goals, team, roles and responsibilities, and allocated tasks, it is time to understand the basics of the organisation. This step is where the customisation to the airline business occurs: it is about the identification of the airlines' specific market environment, the strategy it pursues in that market, regulatory issues emanating from national, paranational and international bodies, its value chain and supply chains. These cover both internal perspectives of the company and external elements related to suppliers and partners. Knowing these elements will help understanding how risk averse the airline is and identify its risk maturity level, not only based on the internal information collected, but also on the input received from external entities. This will also help defining the airlines' risk appetite.

Figure 118: Framework Step 1 – Set basics

Each of these elements will be addressed in detail below.

7.3.1.1. Strategy ID

Recalling, the definition of risk according to the ISO 31000 standard is the "effect of uncertainty on objectives". Therefore, to manage risks one must know the objectives the organisation wants to achieve, as each risk may affect one or more of these objectives. Moreover, to set a proper risk management strategy and define goals for the risk management function, one must know the corporate strategy and goals, and make sure they are aligned. Therefore, this element is probably one of the most important ones when it comes to setting up a new risk management function.

Assuming that the airline already went through a strategic planning process, essential base information should be readily available. This therefore involves:

- Collecting the airlines' mission statement, overall vision, goals and corporate values. This shows what the airline is or wants to be, when and how. It is normally contained in the Strategic Plan and/or Business Plan and should show pre-defined quantified targets.
- A strategic direction should be available, showing how the airline wants to achieve its goals. If not available or documented, outline one based on interviews with key stakeholders, internal management workshops, etc. Without a corporate strategy it will be difficult to design a risk management strategy, risk tolerance and attitude.
- Understanding how all available resources are being combined – or how should they be combined to fulfil the strategy the airline has outlined? Is this working properly or should amendments be made?
- This step should also include thorough SWOT[26] and PESTEL[27] analyses – to complement and prepare the elements of the following steps. A SWOT can be a useful tool to highlight internal issues related to the companies' strengths and weaknesses, while also stressing the external opportunities and threats. The PESTEL analysis provides a broader view of key issues in the surrounding environment and how the organisation positions itself against them.

Analysing the airlines' Business Plan, Annual Results, Budget reports or even detailed Route Profitability reports, for example, from a risk perspective may highlight issues that are otherwise not looked at. Is the Business Model resilient enough? Are there enough defence mechanisms foreseen in the Business Plan that will help overcome over-optimistic assumptions and compensate for revenue streams below plan? Does the Business Plan enable the achievement of strategic objectives or is there anything that can affect its achievement? Are our routes sustained profit makers at all levels, or not?

[26] Strengths, Weaknesses, Opportunities, Threats
[27] Political, Economical, Social, Technological, Environmental, Legal

Recalling input given by some interviewees, a risk can be anything that affects the fulfilment of the Business Plan. Knowledge thereof is essential in order to design a proper approach to managing risk.

If none of these elements are available, they should not be developed within the risk management exercise, but as a parallel and stand alone effort due to their diverging objectives, tools and resource requirements. Nevertheless, the risk management exercise should not be suspended until these documents are available: the airline must keep on flying, the business continues to exist.

7.3.1.2. Stakeholder ID

An airline, as any other company has a set of internal and external stakeholders with whom it is in direct and constant interaction. These can be clients, suppliers, regulators, state, shareholders, employees, competitors or any other category that has some kind of business, interest or participation in the daily life of the airline. Each of these stakeholder groups have their own requirements and expectations, take decisions and act in the market place in a manner that can impact a companies' life. Identifying who they are, what they want, how they can impact an airlines' operation, and establishing a close communication line with them is the only way to involve each of these stakeholders into the risk management effort the airline is trying to introduce.

From an airlines' perspective, are not only regional and national authorities relevant (that negotiate air service agreements and overflying rights, grant operating licenses, establish safety regulations), but also all companies (that act as suppliers) and the general society (that is impacted by the airlines' operation and expansion at the local airports) of where the airline is based, and of all the destinations it flies to and overflies to get there – it is a truly global business. Stakeholder groups of each location have to be taken into account, therefore the best would be to conduct stakeholder analysis exercises for each of the locations the airline serves.

Associated to this is the management of these stakeholders and their expectations: who communicates with each stakeholder from our own organisation? Is there a direct communication line? How can we address their requirements? How can they affect our operation?

A recent example of this interaction refers to the operation of TAP Portugal into Guinea Bissau, a former Portuguese colony in Africa. TAP was the only European carrier flying into that country until the airline was forced to suspend the route after a minister of the local government directly mandated – against the will of the airline and local airport security officers – the embarkation of a group of Syrian refugees holding illegal documentation, facing the threat of seizing the aircraft, crew and passengers in Guinea Bissau. The airline eventually took that group of people aboard the plane, but breached international rules by accepting passengers without valid travel documents. Not only was the airline at risk of being fined a financial penalty for carrying these people, but it also had to suspend regular air service to Bissau due to this – now diplomatic – incident between the two countries. Due to the suspension, TAP had to find an expensive alternative way to reroute passengers booked to Bissau and lost future revenues by suspending this destination from its network. This event originated by the intervention of a stakeholder and had impact on the airlines' objectives. The airline could not control the event; it can only try to minimize the consequences by involving the Portuguese diplomatic and governmental authorities.

7.3.1.3. Market ID

This topic addresses the airlines' competitive positioning in the market. It is about competitors, customers and the airlines' own position in this landscape, in a mix of strategic and commercial issues. Key questions include:

- Who are the airlines' competitors?
- What are the strategic differentiators and competitive advantages of this airline against its competitors?
- What is the airlines'/the competitors' relative market share in each market served?
- What development plans do they have?
- Who are current and potential partners?
- What merger & acquisition movements are going on – are we predators or prey?
- How large is the customer base by market?
- Do we serve all market segments or focus on just a few?
- How does the airline position itself in the market to attract (and serve) our customers?
- Do we have subsidiaries that act in other markets? How are they integrated with the airlines' business and how are they positioned in their markets?
- Can these subsidiaries produce risks that impact the shareholding organisation?

Answers to these questions can and must be provided by the Strategy Development and Commercial Planning functions, hoping of course that the airlines' resources are capable of

providing enough insight into these issues. Benchmarking exercises with best-in-class and peer airlines could be a useful tool to produce quantitative information, beyond qualitative statements gathered in internal interviews to key managers.

7.3.1.4. Compliance ID

As mentioned earlier, air transport is probably one of the most regulated industries. National, regional, international bodies all issue more and new rules and regulations to control operations, safety and sustainability. Examples include national civil aviation authorities, the International Civil Aviation Organisation, the International Air Transport Association, the European Agency for Safety in Aviation, the Federal Aviation Administration. Airline managers are nominated postholders and accountable managers and face legal action if regulations are not complied with. On top of these come market regulators (such as the US-based Securities and Exchange Commission) if the airline is listed at a share market, local and international competition authorities and courts in case the airline is in breach of competition rules potentially leading to heavy fines or operational restrictions. Addressing these issues from a risk perspective enables asking a number of questions:

- Are we aware of and compliant with all these rules and regulations?
- What are the implications of non-compliance?
- Do we have a formal unit to manage all compliance-related issues?
- Who represents us at these bodies?
- Can we influence the decisions and rules taken by these bodies?

Many more questions can be asked, of course, but all must be addressed by the respective legal and operations departments in charge of handling the issues. From a risk management perspective, it is relevant to highlight issues, ask about compliance, register actions taken and know who the right internal counterpart is in case of further need.

7.3.1.5. Value Chain Analysis

The case of the typical airline value chain (where risk management is traditionally absent) has been explored before. Each airline has its ways to organise itself and thus a different – more or less complex – value chain. Mapping out all elements in this chain, describing current processes and the ideal situation will help identifying and managing potential gaps and shortcomings that can result in risks to the organisation. This should include outsourced operations, the legal and contractual aspects related to those outsourced

activities. Having clearly assigned roles and responsibilities for each of the tasks enables quicker decision making and communications.

If each department knows its function within the entire organisation, it will be more capable of engaging in its own tasks knowing the relevance and importance for the airline. Communication, empowerment and engagement should not be nice buzzwords, but part of the airlines' philosophy throughout the entire organisation, both at horizontal levels and vertical lines of reporting.

Part of this could be the identification of the corporate culture (linked to the strategic goals and corporate values) set out in the Strategy ID step. If safety is truly embedded in the everyday business and each employee works with a zero-accident mindset, related risks are naturally reduced and mitigated.

7.3.1.6. Supply Chain Analysis

The introduction delay and subsequent operating problems of the Boeing 787 Dreamliner, and the impact this had on airlines, is a great example of how problems in the supply chain can affect its growth and development plans. While every new product introduction is inherently associated to potential problems, the number of delays, problems and costs incurred with this aircraft in particular caused problems at many airlines – and at Boeing. Air New Zealand's CEO statements, on the 787 delays as being the most critical issue for the airline in that year, have been quoted before. The impact of these delays in the recovery of Japan Airlines was also visible, with new routes postponed as existing aircraft were too large and/or not economical for that particular route.

Of course one airline cannot control issues arising in its supply chain, but it can try to find ways to mitigate potential problems. Keeping the aircraft example, some airlines consciously choose to order aircraft from multiple manufacturers in order not to be dependent on one alone (apart from profiting from earlier delivery slots from both manufacturers, if the airline wants to grow quicker than one single manufacturer can supply capacity). Contractual penalties can also be included; while not solving the core issue, it may cover the financial impact of finding an alternative solution.

The suggestion is to build up a catalogue of current and potential suppliers, containing information on what their part in the airlines' business is, how they manage risks, and how they can affect the airlines' operation. Understanding the dependency of the airline on one

of these suppliers, may help mitigating potential risks, by distributing orders over more than just one supplier. Recent aircraft orders by single airlines but split among various manufacturers is a good example of such a mitigation strategy. This comes of course at a cost, as bargaining power and critical mass may get reduced, and the complexity of managing multiple supplier contracts increases. In any case, knowledge is power, and knowing where the airline stands against its supply chain is the key issue here.

Therefore it is suggested, for the most critical items, to establish partnerships either between similar client organisations in order to increase purchasing power (thus reduce costs) or with alternative suppliers to face potential disruptions.

Taking risk management a bit further would imply suppliers managing their risks according to same (or similar) standards, too, in order to have total alignment. This might be part of the vision presented earlier of a truly integrated risk management effort.

7.3.1.7. Risk Maturity Definition

This element involves the application of the concepts presented in section 2.4.2 “Identifying an organisations’ risk maturity”, aiming at identifying where the organisation, in this case airline, sees itself in terms of risk maturity. One could use the risk maturity model as suggested by Baxter, based on the *capability-maturity-model-integration* model, using the five categories ‘Strategy, Team, Process, IT and Culture’ (as seen in Figure 18); the one proposed by the IMA (Figure 20) or a questionnaire to key airline managers and directors like the one suggested by Brodeur and Pritsch of management consulting firm McKinsey & Co (as seen in Figure 21).

The goal is not only to identify the airlines’ maturity level at the starting point of the risk management exercise – presumably low – but then also to have a comparison value for repeat maturity surveys after the risk management exercise has been implemented.

7.3.1.8. Risk Appetite Definition

Defining risk appetite is about setting the boundary of what is and what is not acceptable for the organisation. Creating such a threshold will make it easier to eliminate risks that fall beyond that level, focussing and prioritising risks that fall within the acceptability range. The best and probably first practical example of this in the airline world is, as exposed earlier, the Lufthansa case where “major risks are defined as dangers which per se might

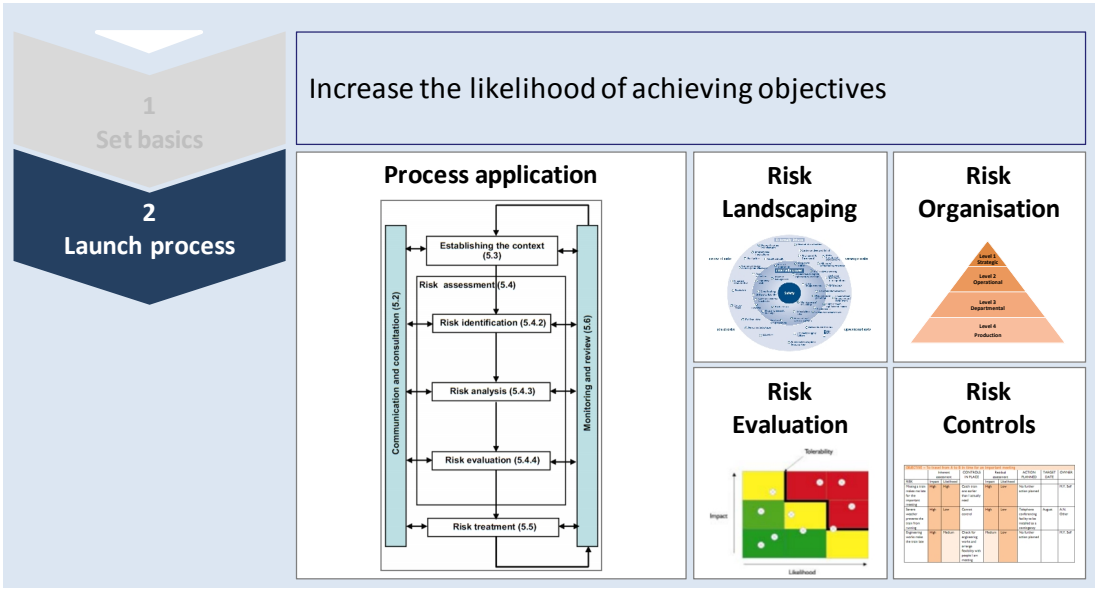
cause damage equal to at least one third of the result necessary to maintain the Company's inherent value" (Lufthansa German Airlines, 2004, p. 100).

As in the case of the maturity model, there are a number of pre-formulated templates and online resources that can be used for establishing this risk appetite level. Section 2.3 "Defining risk appetite" discussed in greater detail how to define risk appetite.

7.3.2. Launch Process

The purpose of launching a risk management exercise is to increase the likelihood of achieving an organisation's objectives. The full deployment of the 'set the basics' elements should enable an easier roll out of the ISO 31000 risk management process: the internal and external conditions are now clear, compliance levels have been identified, the airlines' risk maturity and risk appetite levels are known. This step therefore proposes to apply the original ISO 31000 process, coupled with risk landscaping and evaluation exercises, while also building up an internal risk organisation and set up a risk control portfolio.

Figure 119: Framework Step 2 – Launch Process



The following sections will outline each of these individual elements.

7.3.2.1. Process Application

As described in section 4.2 “Focus on ISO 31000:2009”, the ISO 31000 process foresees seven individual components:

- ‘Establishing the context’, which in this sequence may recapture information consolidated during the earlier steps. Forms and formats for reporting purposes should be defined, involving all participating units to get their buy-in and acceptance. Key Risk Indicators (KRI’s) should be identified, as well as means to measure them, while setting their targets and objectives for the whole process.
- ‘Risk identification’, formally introducing tools to identify risks; tool examples include interviews, workshops, brainstorming sessions. A list of usable tools has been shown in Figure 51: Applicability of tools used for risk assessment.
- ‘Risk analysis’, using the same list and respective tools to proceed to the analysis of individual risks, describe them in detail, followed by
- ‘Risk evaluation’, using heat maps, 5-by-5 matrixes, quantitative evaluations or any other model more suitable for the specific organisation;
- ‘Risk treatment’, focuses on applying mitigation actions to prevent the risk from occurring and/or reducing the consequences of their occurrence if it has negative consequences; or exploit the benefits if the respective risk has positive outcomes.
- In parallel ‘Communication and consultation’, with all entities previously identified;
- ‘Monitoring and review’, to identify process adjustment requirements.

This is a revolving process therefore multiple iterations may be necessary to have a solid list of risks, properly described and evaluated. Forms and formats for reporting purposes should be defined, involving all participating units to get their buy-in and acceptance.

Taking advantage of work performed in the previous Set Basics step, this is the ideal moment to identify KRI’s; set targets and objectives to be achieved, define a realistic time horizon for their achievement and required means to measure them. A KRI can be defined as an indicator that “relates to a specific risk and demonstrates a change in the likelihood or impact of the risk event occurring.” (ISACA, 2010). COSO distinguishes Key Performance Indicators (KPI’s) from KRI’s as being those that “provide timely leading-indicator information about emerging risks” (COSO, 2010, p. 1). Furthermore following core elements are listed as essential for well designed KRI’s (COSO, 2010, p. 6):

- Be “based on established practices and benchmarks”,
- Be “developed consistently across the organisation”,
- “Provide an unambiguous and intuitive view of the highlighted risk”,
- “Allow for measurable comparisons across time and business units”,
- “Provide opportunities to assess the performance of risk owners on a timely basis”,
- “Consume resources efficiently”.

ISO 31000 refers to 'risk management performance indicators' without specifically presenting a definition and/or key attributes of such indicators. In any case, it is mentioned that these should be determined in the "Mandate and Commitment" stage, thus even earlier – at the very introduction – of the risk management framework.

The number and type of such KRI's depends on the organisations' level of complexity and desired depth of the risk management exercise. Examples of such KRI's can include:

- Related to the organisations risk management practices: "Total Risk Exposure", "Number of risk issues that exceed risk tolerance" (KPI Library - ServiceNow, 2014);
- Related to the organisations' business processes: "Customer complaints", "Product Returns", "Overdue Maintenance Orders" (ISACA, 2010)
- Related to the industry: On-Time-Performance, Average Utilization, Average Yield.

Several other papers and articles on KRI definition are publicly available (e.g. (Immameni, et al., 2004); (Institute of Operational Risk, 2010)). The latter goes as far as providing a detailed list of KRIs for financial institutions and, on a more aggregate level, classifies the utility of specific KRI groups for various industries. These KRI groups are concentrated in categories such as 'external threat monitoring', 'incident driven' or 'governance and management control', among others. For the 'Aviation and Transportation' industry it lists almost all as 'very applicable'.

Figure 120: Types of KRI's by industry – focus on aviation

Industry sector	Common operational risk events	Type of applicable KRI									
		Processing error	System performance	Customer service	Staff monitoring	Quality control	Information Security	Litigation	Governance and management control	Incident driven	External threat monitoring
Agriculture	(a) Extreme weather (b) Pollution (c) Quality scandal	Very applicable	Applicable	Applicable	Applicable	Very applicable	Less applicable le	Applicable	Applicable	Very applicable	Very applicable
Aviation and Transportation	(a) Extreme weather (b) Industry accident (b) Labour strike	Very applicable	Very applicable	Very applicable	Very applicable	Very applicable	Applicable	Applicable	Very applicable	Very applicable	Very applicable
Biotech, Nanotech, Life Science	(a) Laboratory accident (b) Intellectual right dispute	Very applicable	Very applicable	Applicable	Applicable	Very applicable	Very applicable	Very applicable	Applicable	Very applicable	Applicable

Source: adapted from (Institute of Operational Risk, 2010), own highlight

7.3.2.2. Risk Landscaping

After identifying, describing and evaluating all risks it should be possible to produce a visual depiction of the risk landscape in a figure similar to Figure 59: Airline Risk Factors, now adapted to the specific case of the airline at hand. It might be necessary to adjust the type and number of categories, for example, or use multiple layers of such depictions for each of the departments or subsidiaries involved in the risk management exercise.

While this does not show any severity or impact levels, it enables the visualisation of the entire risk landscape, showing the most voluminous areas. Safety is normally at the centre of each airline operation – as depicted in the aforementioned figure – but an airline is not safe by decree; all actions need to be taken to ensure consistent safety records.

7.3.2.3. Risk Organisation

In parallel to the above exercise the team mandated to run it should also set up the formal risk management organisation within the airline. They are going to constitute the central risk management unit that is setting the process, defining deadlines and gathering input from the respective units, but they cannot do the entire work on their own. It is therefore required to identify risk champions along the airlines' departments that act as intermediaries and local counterparts for risk management purposes.

As seen earlier, some airlines tend to decentralise risk management, others tend to have a centralised unit coordinating the entire process and directly reporting to the board. This should be decided together with the board that has mandated the entire exercise. Given that there are various levels of risks and there should be the possibility of escalating risks up and downwards in the organisation, it is proposed to organise the airlines' risk response around source and impact (similar to Figure 16: Delegating and escalating risk appetite):

- Strategic risks should be handled by upper management;
- Operational risks are responsibility of senior management;
- Departmental risks are to be managed by middle-management; and
- Production-related risks should be managed by individual operational units.

If any of these risks in a lower department surpasses the airlines' (and departments') risk appetite level, it should be escalated to upper management levels. Communication and empowerment is essential here, as not all risks should be kicked upwards; lower management levels need to be able to decide on how to act on minor impact risks.

7.3.2.4. Risk Evaluation

This element should recapture the individual risk evaluation exercise conducted during the "Process Application" step in order to put together a big picture of all risks and respective evaluation results. Depending on the sophistication and management style of the organisation, a quantitative and/or qualitative risk evaluation needs to take place along aspects of likelihood and impact.

It is suggested to add a third dimension on speed of occurrence, showing that even less likely events – but with high impact and high speed of development – should be looked at.

A general tolerability level is related to the risk appetite limit defined earlier. This should help setting priorities for action taking.

7.3.2.5. Risk Controls

Reporting is key in this process. The more detailed such reports are the easier it will be to track responsibilities on actions taken (or not taken). Ideally such reports are tool-based for easier and automatic handling, avoiding manual typing in preformatted templates and spreadsheets. Predefined risk controls help creating a uniform treatment description and allocate tasks and responsibilities.

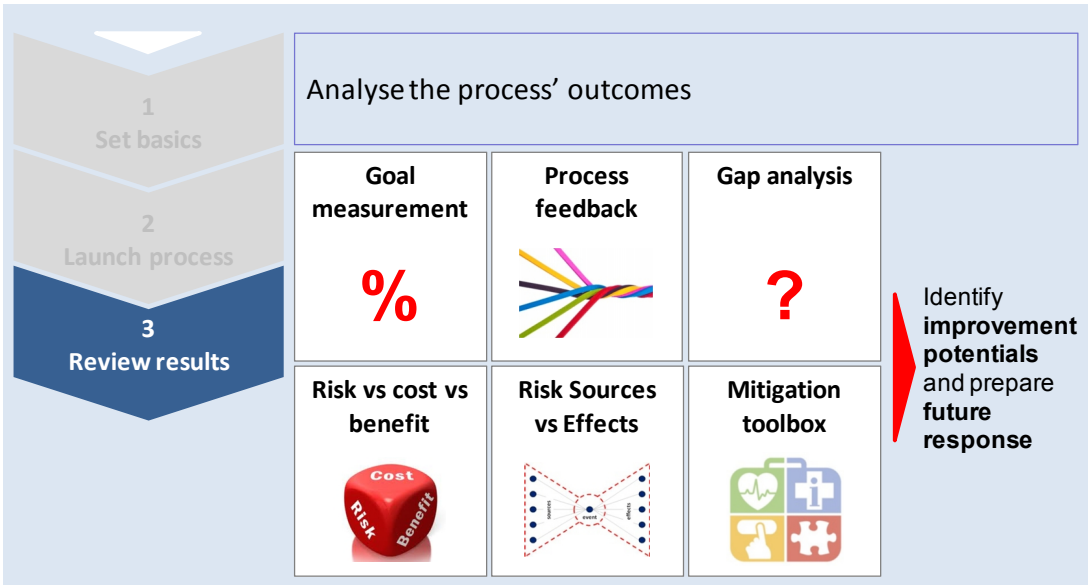
Adding "residual risk assessment" enables the depiction of the risk landscape before and after risk mitigation measures have been implemented. Ideally a left-wards movement on the likelihood-impact graph should become visible after such measures have been adopted.

7.3.3. Review Results

Gordon Song, Tigerair's Head of ERM and Internal Audit, previously quoted from the StrategicRisk Magazine, is blunt: "there is a lot of subjectivity to the old 5x5 risk matrix. (...) When one doesn't sit down and look at the numbers and the root causes of what the risk is, unfortunately you then get very misguided risk management. This leads to action plans that might be convenient to implement, but do little to change the risk profile". Moreover "if the stakeholders do not get any value from the programme, you can bet that the whole risk-management agenda gets downplayed or is completely destroyed after a few short painful years" (Jones, 2013, p. 2). It is therefore important not only to properly analyse – beyond numbers – the identified risks, exposure and controls, but also the overall risk management process itself implemented at the company.

Having these comments in mind this 'Review Results' step has been designed to identify results achieved with the whole risk management approach, as well as the internal process improvement potentials to adjust the organisation and its risk management process for the future. After conducting all elements of the previously described risk management process, it becomes necessary to review the results of its implementation, by comparing KRI target levels with the actually achieved results, gather internal feedback on the process and identify gaps. At this point it should also be possible to reflect on the investment required to manage and mitigate all identified risks, as well as the number and type of risk sources and potential effects they have on the operation. Finally the airline should be able to congregate all information produced on risks, possible controls, their effectiveness, key counterparts for each risk and other elements to build the airlines' own and specific risk mitigation toolbox. All these individual elements are further described below.

Figure 121: Framework Step 3 – Review Results



7.3.3.1. Goal Measurement

This is a self-explanatory element of this risk management approach: KRIs have been set earlier, it is now time to collect data for each KRI that enable concluding on its achievement. To complement this, if and wherever possible, a benchmarking exercise should be launched using other airlines (partners, regional peers or best-in-class), alliances, or the whole industry (if data is harmonized and available) for comparison purposes.

As soon as these results are collected, it will be possible to identify shortcomings and/or areas where targets have been over-achieved.

7.3.3.2. Process Feedback

This step foresees the collection of formal and informal feedback on the risk management process and its effectiveness. Therefore it requires input from all internal and external contributors. This input can be gathered via one-to-one conversations, structured interviews, anonymous feedback forms, group workshops, company-wide surveys, etc.

During this process missing items and weak areas requiring adjustment will be identified, that can ultimately lead to improvements of the process, the risk landscape, the mitigation measures put in place, resource allocation, responsibility assignment or any other element of the risk management approach.

7.3.3.3. Gap Analysis

The previous two elements ('Goal Measurement' and 'Process Feedback') enabled understanding the achievement of planned results, comparing these against the pre-defined goals and KRIs, as well as looking at other organisations, while gathering feedback on the process. All this contributes to the identification of possible gaps in the process and its outcomes.

Therefore, it is relevant to know:

- What is missing?
- Why is this happening?
- Can the process be adjusted?
- What has to be changed?
- What is needed to change it?
- How long will it take?
- Will the change be effective?

Answers to these questions will help building a process improvement plan that is targeted at correcting uncovered shortcomings.

7.3.3.4. Risk vs Cost vs Benefit

A cost benefit analysis to the key risks, their mitigation measures (and costs associated to these measures) and expected benefits should be conducted to understand if it is economically sensible to invest in controls that ultimately reduce little in the risk exposure.

This exercise should not be conducted solely by the risk owners, as their perceptions might be skewed (every risk must be mitigated, regardless of their impact). Instead, it should be coordinated by the risk management unit, getting help from cost-benefit experts in the organisation (e.g. economic studies) and/or other third-parties to get their external views on the issue.

While the result of this should not be a go/no go decision to mitigate or not each identified risk, it should rather highlight the involved costs of mitigation, expected benefits (or avoided losses) to the risks that have been identified and addressed.

7.3.3.5. Risk Sources vs Effects

For the identified risks (at least for those considered top priority) it is relevant to understand what are the triggers contributing to its occurrence and check the effects that this might have within or around the company. Plenty of the literature quoted in previous chapters (e.g. (COSO, 2010)) refer to 'root causes' at the origin of events or intermediary events that can result into the actual risk. Establishing these interdependencies and correlations between different risk events, sources and their effects can help the organisation in properly addressing future issues and identify at an early stage possible root causes – and thus prevent events from happening and becoming risk events. To help visualize the complexity of the risk landscape, the interdepency of the various risks and their sources, a graphical depiction of all risks, sources and effects could be produced. This effort helps streamlining the whole risk landscape and reducing it to the core essential elements, eliminating duplications and redundancies.

7.3.3.6. Mitigation Toolbox

The purpose here is to collect all possible risk mitigation measures introduced during the whole process, complementing this with other potential measures that have not yet been used, but are available and dominated by internal staff. This will build a catalogue of possible mitigation measures that are available upon request.

If possible, include feedback on the mitigation measures, outlining effectiveness, ease of implementation, speed of mitigation, etc.

As soon as this is compiled, it can be disseminated among responsible staff, risk champions and included in risk trainings within the organisation for future reference and use. Of course, to keep its validity, it must be constantly reviewed and updated by the central risk management unit in charge of the whole risk management exercise.

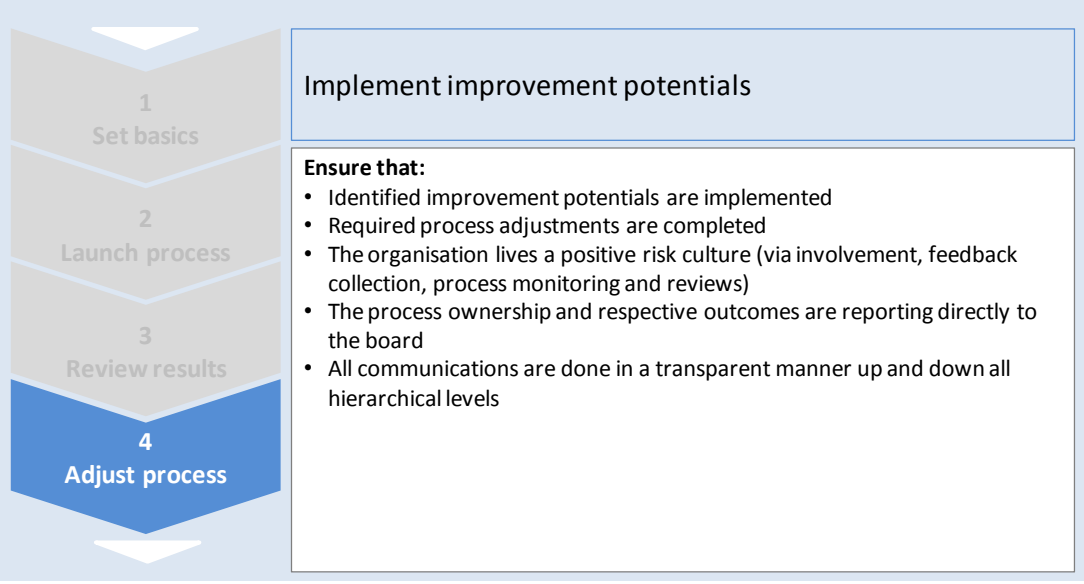
7.3.4. Adjust Process

Now that a number of improvement potentials have been identified, it is important to implement necessary changes. For this, it must be ensured that:

- Required process adjustments are completed,
- The organisation lives a positive risk culture (via involvement, feedback collection, process monitoring and reviews),
- The process ownership and respective outcomes are reporting directly to the board, and that
- All communications are done in a transparent manner up and down all hierarchical levels.

The iterative character of the whole framework will automatically take the risk management process to revisit the first steps and continue with risk identification and evaluation exercises.

Figure 122: Framework Step 4 – Adjust Process



7.3.5. Tentative timelines

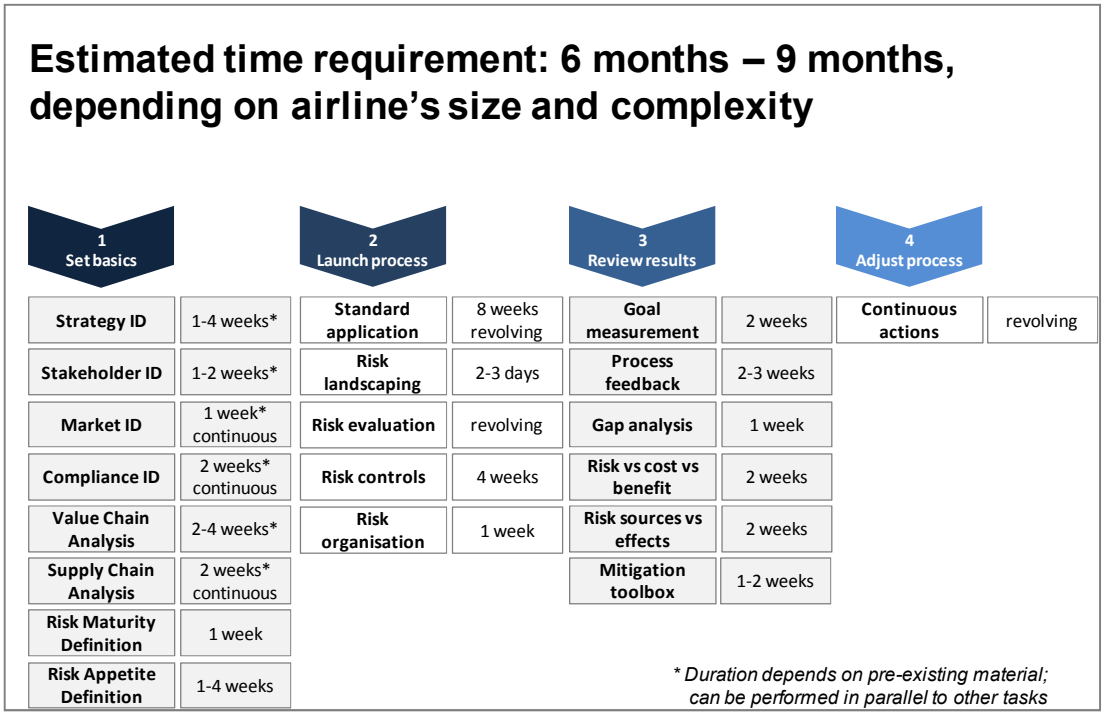
All the above seems to be quite voluminous in terms of work, involved people, interdependencies, etc, but the actual time needed to set up the whole process depends on the organisation's size and level of complexity. For example: strategic elements for the 'Strategy ID' step might be readily available, thus it is not required to spend time producing these; it is 'just' about its analysis from the risk management perspective. The same happens with all other elements.

As discussed, the whole framework proposal can be (and must) customized. Recalling, not even the ISO 31000 that is used as base is certifiable exactly because it must be adjusted to each specific organisation and industry.

So how much time is required for a medium-sized airline? It is estimated that implementing the whole process and running the first iteration, with all its elements, may take between 6-9 months, depending on the airlines' level of readiness.

The next figure lays out a tentative time-scale for all steps.

Figure 123: Tentative time-scale for framework implementation



This timeframe – possibly quite ambitious in its depth and too aggressive in terms of goals – shall be object of validation with airline representatives in the next chapter of this thesis.

7.4. Chapter Summary: what is new about this proposal?

The above sections laid out a proposal for adaptation of the ISO 31000 framework to the airline environment. While being an industry-neutral standard, this proposal includes industry-specific elements in an attempt to facilitate understanding concepts and ultimately improve the use of ISO 31000 within the airline industry. As seen in previous chapters ISO 31000 is still one of the least used risk management standards among airlines.

In summary, what are the key advantages of this proposal for adaptation? What is new about it? The following independent topics can be listed:

1. The proposed framework is adapted to the airline environment, thus bringing in industry-specific elements into the industry-neutral risk management framework.
2. It is based on ISO 31000, the latest and most widely accepted risk management standard that considers risk from its positive and negative angles.
3. The proposal clarifies concepts and language used in ISO 31000, making it easier to implement in the airline industry.
4. It is a customizable framework to any airline size or level of development. Some other standards are hermetic and less flexible to customization.
5. This proposal reinforces the key business aspects of the airline – as a business, not just a flying operation – thus being holistic, covering business specific and operational areas.
6. It involves all departments of the airline, thus the entire value chain, as well as key stakeholders into the risk management effort, making risk management a constant and ever present priority for all.
7. It helps risk management units gaining visibility within the airline.
8. It improves the airlines' resilience by making it better prepared to face risk events and identify respective root causes.
9. It helps the airline achieving its objectives and reducing the daily risk in their operation.
10. Unlike other standards, it proposes a time-frame as guideline for each of its steps and core elements.

But is this proposal feasible? Would it be accepted if presented to an airline willing to introduce risk management? Is the proposed timeframe too aggressive? To answer these questions the entire proposal has been submitted to a validation process by risk experts and airline representatives. The next chapter will detail the methodological aspects of this validation process, results achieved and proposal improvement potentials gathered from that process.

8. Proposal validation

As stated in the early chapters of this thesis, the project intended to be as close to the airline industry as possible, not only by identifying current ways of handling risk management at airlines, but also by proposing changes that could bring added value to the industry. The previous chapter described a proposal that adapts an industry neutral risk management framework to the airline environment. While being based on risk management best-practice, it still needs to be tested for its usefulness within the specific airline industry. Having this in mind, the present chapter describes the validation process and the results achieved.

8.1. Methodological approach

One way of proceeding with such a validation exercise would be to apply the proposed adaptation to airlines that were willing to introduce risk management. This would not only require the willingness of one airline (at least) to implement risk management following the proposed framework adaptation, but also the necessary time to implement, review, adapt, correct and improve results achieved. Given that no airline was receptive to such an undertaking and that the whole process could last – at each participating airline – several months, or even years as per some interviewees' suggestions (see Chapter 5 Current Risk Management practices at airlines), and that this would just reflect the views of each individual airline, a more efficient approach to the validation process needed to be chosen.

In order to gather more substantial input in a time-effective manner, several airline risk managers and experts have been invited to provide direct feedback on the proposed framework adaptation. For that purpose the previously outlined framework adaptation has been summarised in a presentation-style document (see Annex D), distributed to the selected experts and these have all been asked four questions on the usefulness and validity of the proposed framework adaptation.

The criteria to choose experts to participate in this validation process were to have experience at airline risk management functions (current or previous) and/or have airline management experience with significant exposure to risk management. Taking advantage of contacts established during the interview process, some personalities were now re-invited to validate the framework adaptation. They were already briefed about the project's scope and goals and showed previously willingness to cooperate further.

Of the fourteen invited personalities, seven provided full replies: five are current or former airline risk managers and two are higher level managers with significant risk management exposure. The figure below summarises names and positions of participating experts.

Figure 124: Validation Process participants

Validation Process

Participating experts
(with validated replies)

With airline risk management experience (from current or former positions)…	**With airline management experience and exposure to risk management issues…**
▪ **Mr. Ólafur Briem** Director Risk Management Icelandair Group ▪ ***undisclosed*** Director Risk Management, Large German aviation group ▪ **Mr. Steve Tunstall** former Head of Corporate Risk Management, Cathay Pacific now Vice President Risk Management at Genting Singapore ▪ **Mr. John Dombrick** former Head of Entreprise Risk and Business Continuity British Airways ▪ **Ms. Elaine Liew** Risk practitioner and trainer, former Manager Strategic Risk Management Unit Malaysia Airlines	▪ **Mr. Yevgen Treskunov** EVP Strategy & Development, Ukraine International Airlines ▪ **Mr. José Castellanos** VP Aviation Division QSL Consultores – IATA strategic partner for Risk Management – currently General Coordinator for Quality, Safety and Security for TAAG Angolan Airlines

These personalities were asked four questions designed in a way to collect concise opinions on the framework adaptations' effectiveness, usefulness, stakeholder buy-in and timeframe suggestions. While not being representative of the entire industry, the variety of participants (by airline size, geography, business model, etc.) enables capturing feedback from different perspectives. All answers provided are detailed in the following section[28]. The questions were:

1. How would the proposed framework enable your airline to achieve a more effective risk management process? If not, why?
2. Would you consider using elements of the framework (in full or just some elements) to improve the risk management process at your airline? If yes, which elements; if no, why? Or would you consider this framework to be more useful for airlines just about to start their risk management efforts?
3. Is it realistic to aim at getting the buy-in of all stakeholders in the risk management process, so that the entire industry becomes more risk aware, or is this an unachievable goal? Please elaborate.
4. Do you think it is possible to implement a risk management process based on such a framework within the proposed timeframe (6-9 months, depending on airline size and complexity) or does any element need to be adjusted?

[28] Mr John Dombrick did not answer the four questions individually but in one global answer. His contributions will not be listed separately but referred to whenever appropriate.

8.2. Validation questions

Answers to each validation question will be addressed separately below. Each contribution reflects the participants' individual opinions only, not compromising the airlines they work for or have worked for in the past. For transparency reasons, original answers have been transcribed into a standard table that for each question shows their respective answers.

8.2.1. Validation Question 1: …on the effectiveness of the framework adaptation

The first question aimed at assessing the participants' opinion on the proposed frameworks' effectiveness. It has been formulated as: "How would the proposed framework enable your airline to achieve a more effective risk management process?" To complement this, assuming that some could reject the effectiveness of the framework, participants were also invited to answer "If not, why?"

The general feedback was positive, with most of participants recognizing the value of the proposed framework adaptation, classifying it as effective if it would be implemented at their airlines. One participant highlights the need for customization, criticizing the lack of a holistic approach in specific operational, commercial and support processes. Another participant points out the lack of guidance for quantitative risk management methods. These criticisms shall be addressed below.

Table 4: Validation Process: Answers to Question 1

Participant	**Question 1:** "How would the proposed framework enable your airline to achieve a more effective risk management process?"If not, why?"
Mr. Steve Tunstall former Head of Corporate Risk Cathay Pacific / Swire Group	"The framework provides a useful and concise summary of a useful risk management methodology for an airline. It is helpful to have a comprehensive guide as a reference point and would be useful for validation of existing processes and identifying any potential gaps."
Mr. Ólafur Briem Director Risk Management Icelandair Group	"The proposed framework is more formal and exhaustive than the one we follow. Our framework is based on COSO but is limited to evaluating the financial impact on the projected cash position 12 months forward. I see for example that encompassing the KPI´s as suggested in the proposal would broaden the concept we currently are dealing with. So would the definition of stakeholders which is non-existent in our framework. We haven´t explicitly connected our ERM to the corporate mission

	statements/vision/values although we have urged the team members to base the ERM process on SWOT analysis. Further, the proposed framework underlines the importance of standardized reporting which is a method which we could improve. The only drawback I notice is the lack of guidance as to how to evaluate VaR, ie probability and financial impact of shocks which needs to be standardized across the units."
undisclosed Director Risk Management, Large German aviation group	"At this point in time it wouldn't, as this company has been evolving its own risk management processes along very similar guidelines over the past years. (...) We haven't applied ISO 31000 – or any other risk management standard in particular – rather collected valuable aspects of each available standard and coupled these with the needs and requirements of our own organisation. (...) Nevertheless the proposed approach is logically structured and makes sense, possibly more for airlines just about to start their risk management efforts than for companies that are involved with it for a long time."
Mr. Yevgen Treskunov EVP Strategy & Development Ukraine International Airlines	"This will be used as checklist to ensure our current risk management does not miss anything. Also it is a helpful guideline for integration of risk management efforts across the organisation."
Ms. Elaine Liew Risk practitioner and trainer, former Manager Strategic Risk Management Unit Malaysia Airlines	"Some of the items highlighted can definitely be used as potential continuous improvement initiatives for the respective companies."
Mr. José Castellanos VP Aviation Division QSL Consultores – IATA strategic partner for Risk Management – currently General Coordinator for Quality, Safety and Security for TAAG Angolan Airlines	"The proposed framework is only proposing to use the Risk Management Process based on ISO 31000, which I believe is the best option for risk management. The framework does not have a holistic approach since airlines need to analyze risk based on operational, commercial and support processes using one framework. The framework needs to be defined in terms of: • The process to be used (in this case the 7 steps process from ISO 31000) • The entities (areas, processes or geographical scope) and • The elements impacted. In the framework sent I only see the 7 step process."

Regarding the criticisms made on the lack of guidance for quantitative risk management methods, this is true, although very little guidance on any sort of specific methods has been given, being these qualitative or quantitative. The purpose of the whole thesis was not to test the applicability of specific methods, rather to propose a broad and holistic framework based on ISO 31000 where those individual methods can be used, depending on the airlines' specific needs and knowledge to work with whatever methods are most usable. In summary, this framework adaptation proposal was not meant to be a user guide for Value-at-Risk (VAR) calculations or any other quantitative methodology (for which there are plenty textbooks available), but a guideline for airlines to introduce risk management in their organisations.

As for the suggestion that the framework does not have a holistic approach, as individual processes (operational, commercial, support), entities and respective elements are not considered. This is also true and valid, yet on several occasions it has been mentioned that this thesis and respective framework adaptation was aimed at introducing risk management across the entire value chain (including all operational, commercial and support processes), highlighting the need to include specificities of these fields if and when necessary. The initial project objectives also stated that no individual risk factor or origin would be considered in particular, as means to avoid being biased to one alone – say safety or fuel price development – instead of the bigger picture.

Mr. John Dombrick, former Head of Entreprise Risk and Business Continuity at British Airways, stated that, despite having left that airline some years ago, "the ERM structure and methodology has not changed very much". Nevertheless he sees the implementation of this framework at his airline as unlikely: "Given that BA had an ERM process in 2008 that was on a par with any other airline and superior to most (…) it would not necessarily want to migrate its ERM structure to comply with ISO 31000 unless there was some externally compelling influence that drove it. (…) On the other hand, if an airline was seeking a risk management structure then I think ISO 31000 is a good one to adopt but unless they were cash rich or subsidized by their national government I think they would try to adopt the structure without actually going for documented compliance."

8.2.2. Validation Question 2: …on the usefulness of proposed framework adaptation

Participants were invited to answer following question: "Would you consider using elements of the framework (in full or just some elements) to improve the risk management process at your airline? If yes, which elements; if no, why? Or would you consider this framework to be more useful for airlines just about to start their risk management efforts?"

Some very interesting contributions have been received, indicating that the proposed framework adaptation would probably be more useful for airlines wishing to start a risk management exercise, rather than for those who have developed their own approaches over time. The tendency is that established airlines with risk management in place already address some or most of the topics covered by the adapted framework.

The most relevant answers are included in the table below.

Table 5: Validation Process: Answers to Question 2

Participant	**Question 2:** "Would you consider using elements of the framework (in full or just some elements) to improve the risk management process at your airline? If yes, which elements; if no, why? Or would you consider this framework to be more useful for airlines just about to start their risk management efforts?"
Mr. Steve Tunstall former Head of Corporate Risk Cathay Pacific / Swire Group	"Many of the elements set out in the report are already in place at Cathay Pacific where I was previously employed in a role that could adopt this type of system. I guess areas where all risk systems need to be improved include 'risk vs. cost vs. benefit' and serious 'goal measurement'. These aspects are notoriously difficult to quantify from a business perspective."
Mr. Ólafur Briem Director Risk Management Icelandair Group	"I would be inclined to regard this framework equally as useful for airlines whether already involved in risk management or at the very early stages of implementation. I would consider using most of the elements to support the ones lacking in our current effort to reduce risk. The framework sets clear guidelines and ambitious aims and requires considerable resources and many "hands on deck". To embrace all elements and implement the framework as a whole would necessitate very convincing leadership from the Board and executive management. These people would have to be very dedicated, patient and with a long term vision to

	successfully follow this through to such a comprehensive extent. Whether some elements of the proposed framework are realistic is wholly uncertain. For example, I think it is a formidable task to reach out to all stakeholders and define their sets of values but I am sure airlines might proxy that with assumptions via good intentions. Also the element of analyzing and evaluating the inter-correlation between risks or events regarding the "risk resources vs. effects". Without doubt that may be approached in some way."
undisclosed Director Risk Management, Large German aviation group	"The proposed framework adaptation seems to be more valuable for newcomers to risk management."
Mr. Yevgen Treskunov EVP Strategy & Development Ukraine International Airlines	"At UIA we rather will compare the existing approach with the suggested framework. Most probably at the first instance certain elements will be added, as a major revision of the currently acceptable system might require long time for implementation and loss of integrity of the current systems during the implementation stage. Definitely start-up carriers or the airline that just starts risk management implementation could be successful in using the suggested framework. The latter covers all areas of airline activities, provides a single approach to terminology across the organisation and thanks to well prepared check-list allows to securing completeness of the risk management process, as well as its implementation within limited period of time."
Ms. Elaine Liew Risk practitioner and trainer, former Manager Strategic Risk Management Unit Malaysia Airlines	"My overall answer is that I can use some of the elements in this framework to improve the risk management materials that I currently use."
Mr. José Castellanos VP Aviation Division QSL Consultores – IATA strategic partner for Risk Management – currently General Coordinator for Quality, Safety and Security for TAAG Angolan Airlines	"At the moment I am using the ISO 31000 process in the whole airline to understand risk in behalf of quality (compliance), safety (risk related to damage under control) and security (protecting company assets including people from illegal interference)."

8.2.3. Validation Question 3: …on getting the buy-in of all stakeholders

The question asked referred to what was presented and discussed in section 7.1 Goals and vision and Figure 116: Vision of an holistic risk management approach in the airline industry. Therefore participants have been invited to comment on the following "Is it realistic to aim at getting the buy-in of all stakeholders in the risk management process, so that the entire industry becomes more risk aware, or is this an unachievable goal? Please elaborate."

The majority of answers received referred to this as a desirable goal, but stress the hurdles that need to be overcome to achieve it. Some refer to diverging objectives of involved stakeholders, some to the need to streamline internal processes before involving external counterparts.

Detailed answers are included in the table below.

Table 6: Validation Process: Answers to Question 3

Participant	**Question 3:** "Is it realistic to aim at getting the buy-in of all stakeholders in the risk management process, so that the entire industry becomes more risk aware, or is this an unachievable goal? Please elaborate."
Mr. Steve Tunstall former Head of Corporate Risk Cathay Pacific / Swire Group	"It is certainly desirable to get all stakeholders to buy in to the RM process though this can be difficult for a number of reasons. Firstly, most corporate risk processes are dominated by data and bureaucracy. This means that they become historical audit chains rather than living documents where buy in can be realistically sought. Second. The aviation industry has spent decades beating up suppliers in a chase for the bottom on cost, often an unintended side effect has been the impact on quality aspects that cannot always easily be identified. A clear example would be in the area of ground handling. Drivers of equipment worth 250k spend 12 hours a day driving around hulls worth 100m and yet there are many anecdotal stories of the drivers then leaving to get better paid jobs at, for example, McDonalds. Engaging said driver as a key stakeholder in a RM process is perhaps always doomed to failure."
Mr. Ólafur Briem Director Risk Management Icelandair Group	"(…) this is quite uncertain, but I am optimistic that with time it is possible. Already airlines are extending their role as responsible enterprises for the greater good. This can be reflected through HR, their attitude with regards to the environment and local

	appearance/image. This is no coincidence. The industry is growing and affects the life of all people. Airlines are under pressure from local authorities and politically in a global sense as well. Therefore ERM has increased in value for each airline, not just to reduce earnings volatility but also to signal good intentions the stakeholders to accomplish acknowledgement."
undisclosed Director Risk Management, Large German aviation group	"While this is a valid ultimate goal, we first need to have an integrated internal approach before involving external elements. So what we are working on is to have each functional division feeding into the centrally developed risk management system, but they are responsible for interacting with their internal and external counterparts. It is not the responsibility of the central risk management function to gather views and comments on each risk factor from all possible stakeholders. Neither is that our function nor do we have the resources to handle all those stakeholders. It is thus important that all internal functions work according to the same risk management principles, approach and standard. It is possible that most companies haven't yet achieved a level of full internal integration when it comes to risk management. As mentioned above, our model has been and is constantly evolving, and I believe we have achieved a good level of maturity that can take us to the next stage of development. After this first step has been achieved it is possible to advance to the second step, where certain areas can and should cooperate more with their external counterparts. We are in the process of talking to selected partner corporations from similar and different industries to see how they organize their risk management functions and share how we do it. It will be useful to create some common understanding and learn from each others' experiences, while never disclosing sensible information, of course. These discussions can involve applied processes, standards, evaluation criteria, IT support, integration with internal controlling processes, etc. This aims at having an informal exchange platform and will happen at a bilateral basis. We are also in contact with other industries to foster similar exchange platforms."
Mr. Yevgen Treskunov EVP Strategy & Development Ukraine International Airlines	"It is realistic to involve all stakeholders if the Enterprise Risk Management is clearly described and structured as it is proposed in the study. Then each stakeholder can see how his part is affecting the whole company and why it is considered as one of the risks."
Ms. Elaine Liew	"This is the ideal situation which the airline can aim

Risk practitioner and trainer, former Manager Strategic Risk Management Unit Malaysia Airlines	towards. However, from a practical point of view, this will be challenging as the company may have limited sway / influence over its stakeholders (e.g. suppliers, regulators, competitors, state, clients, etc.). To try to achieve this ideal situation, support from a larger entity (e.g. IATA, ICAO) to make risk management a "must-have" or mandated requirement, this can lend some weight to achieve the ideal situation with some of the stakeholders (e.g. regulators, state, etc.)."
Mr. José Castellanos VP Aviation Division QSL Consultores – IATA strategic partner for Risk Management – currently General Coordinator for Quality, Safety and Security for TAAG Angolan Airlines	"It is absolutely necessary to have a holistic approach to risk management that is why we are using a same framework for all the company processes and defining severity characteristics based on impact of people, infrastructure, aircraft damage, environment, service, mission, compliance and safety. We are using a 5x5x5 matrix. 5 levels for Severity, 5 levels for Likelihood and 5 levels for Risk Magnitude and Actions. Each level has a very specific description to avoid subjective approach."

8.2.4. Validation Question 4: …on the proposed timeframe

The suggested timeframe for implementation of the framework adaptation, as presented in section 7.3.5 Tentative timelines, was also subject to review and validation by the participants. The question asked was "Do you think it is possible to implement a risk management process based on such a framework within the proposed timeframe (6-9 months, depending on airline size and complexity) or does any element need to be adjusted?"

The majority of answers received point to the direction that 6-9 months is too tight, as introducing risk management also involves a fundamental culture change within the company and at all employee levels. According to some participants, such an undertaking can take between 3-5 years, and even then it cannot be guaranteed that it is complete. Representatives from smaller airlines seem to lean towards shorter timeframes, but agree that 6-9 months might be too ambitious.

The table below details individual answers.

Table 7: Validation Process: Answers to Question 4

Participant	**Question 4:** "Do you think it is possible to implement a risk management process based on such a framework within the proposed timeframe (6-9 months, depending on airline size and complexity) or does any element need to be adjusted?"
Mr. Steve Tunstall former Head of Corporate Risk Cathay Pacific / Swire Group	"I believe the timescale is unreasonably short to implement a complex and successful business risk management program. Even if there is substantive buy in from senior management (rarely a given) the whole point is about changing the organisational culture. The get genuine acceptance of the language of risk in the DNA of a business culture takes about three to five years, usually at the pessimistic end of the estimate."
Mr. Ólafur Briem Director Risk Management Icelandair Group	"I think it depends on the leadership preference and ambitions. I think it is possible to some extent with the right kind of resources. With reasonable investments in the supportive infrastructure and software for risk registering this should be achievable in a crucial way but possibly not thoroughly. Elements like stakeholders, KPI´s, corporate values, risk reviewing and robust risk registration, need a few cycles for fine tuning. No doubt some elements would be unintentionally left out during the first rounds of ERM processing. Our experience is that the reviewing / repetition process needs to feed through the system a few times to improve the outcome. Creating a sense of culture for risk awareness, doesn´t happen overnight. I would consider that to be the final accomplishment of a successful implementation, apart from the technical and statistical side of ERM. Having established the culture, you have managed to take the task out of the hands of few into the minds of many."
undisclosed Director Risk Management, Large German aviation group	"The question cannot be answered with a simple 'yes' or 'no' as the exact scope needs to be properly defined: are we talking about a small company or a group of companies, what resources are available, are they fully dedicated to this assignment, what is the goal of the project, does it include software implementation (and if yes, how many iteration processes steps do we foresee), etc? Also, introducing such a risk management process requires a fundamental culture change within the company – assuming that no advanced risk management has been performed before. It should not be "you have to manage risk" but "you want to manage risk". At our company we started the development of the risk management approach at the end of 2011 and

	launched the supporting IT platform in July 2012. First results – following the new processes and methodologies – were achieved at the end of 2012. But we are a quite large group with a number business units and subsidiaries. After these two years I can say we have left the "project stage" and can finally consider this a running job with established, mature, recognized and recognizable processes. For an organisation of our size I think 3 years should be OK."
Mr. Yevgen Treskunov EVP Strategy & Development Ukraine International Airlines	"6-9 months is a realistic timeframe for implementing this project disregard of the airline size. After that period any airline will need to have a monthly control and consider adjustments if needed. However these adjustments will reflect first experience and outcomes from using this risk management process."
Ms. Elaine Liew Risk practitioner and trainer, former Manager Strategic Risk Management Unit Malaysia Airlines	"Based on experience, the timeline mentioned above is a little on the tight side. From what I have seen & discussions with other professionals in the risk management field, the timeline can range anywhere between 6 to 24 months depending on the following factors: a) Leadership, involvement and support from top management to implement the risk management process organisation-wide b) Level of hierarchies in the organisation structure c) Size of the organisation d) Organisation working culture e) Skill, competency and commitment of the people involved."
Mr. José Castellanos VP Aviation Division QSL Consultores – IATA strategic partner for Risk Management – currently General Coordinator for Quality, Safety and Security for TAAG Angolan Airlines	"It is realistic to consider a 6-9 months proposed timeframe, only for risk management. We have implemented more than 250 integrated management systems using around 12 to 15 months depending on the size of the organisation for the complete system that includes of course ERM."

8.3. Chapter Summary: findings from the validation process

The validation process was aimed at collecting specific feedback on the risk management framework adaptation proposal as exposed in Chapter 7. Several personalities were invited to answer four questions addressing the proposal's effectiveness, usefulness, stakeholder buy-in and suggested timeframe for implementation. Answers received from airline risk managers and representatives of upper management layers are representative of larger and smaller airlines of various geographical regions and business models.

Following topics can be filtered as summarising conclusions:

- Most participants see the proposed framework adaptation as effective, complete and concise, potentially serving as guideline and checklist for risk management processes already in place or to be implemented.
- The framework adaptation proposal is generally seen as useful for application at airlines, especially as it is based on ISO 31000 as highlighted by some participants, although larger airlines already tend to have similar processes in place covering all or most of the elements included in the framework adaptation. The majority sees this proposal more valuable for airlines that currently do not have risk management processes in place or start-up airlines willing to establish new internal management processes.
- The suggested stakeholder buy-in vision has been considered a good long-term goal, but difficult to achieve in the short-term. First available risk management processes in-house need to be streamlined and improved. Relevant stakeholders need to be identified, in order not to involve even the most insignificant ones. With this in mind, one should not create unnecessary complexity that does not assist in the risk management process' primary goals.
- As for the proposed tentative timeframe, all participants seem to agree that the 6-9 months initially suggested are too ambitious, given that the process involves multiple management layers, departments and redirection (or full creation) of a corporate culture centred around risk management principles. Such a timeframe should to be adjusted to the airlines' size and complexity.

These considerations should be taken on for further development and/or implementation exercises that go beyond the scope of this thesis. Ideally only with a real and hands-on implementation of this proposal at an airline can further gaps and improvement potentials be identified and corrected.

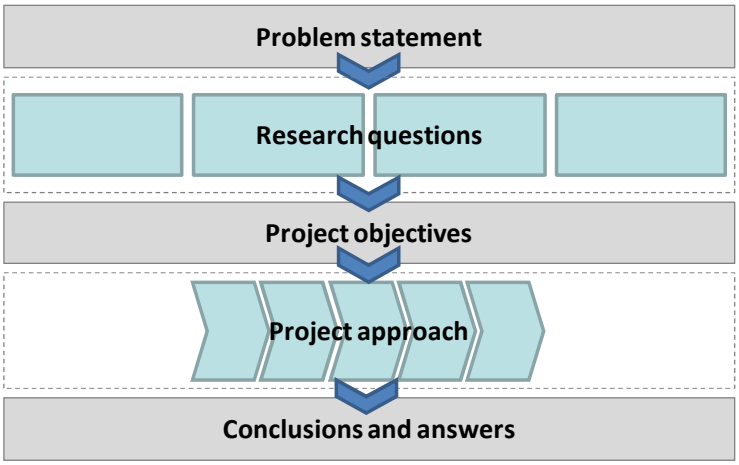
– Intentionally left blank –

9. Discussion of results achieved

Understanding and managing risk as a generic concept and as individual item within a larger risk landscape of an organisation is a journey that requires time and resources. The less familiar organisations are with such concepts, the longer they will need to properly manage each risk and its consequences. Setting up a process that helps addressing risk management in a consistent manner is part of that effort. Airlines are no different. This thesis tried to highlight how airlines perform risk management by identifying current practices, organisational implications and applied standards. The adaptation of one of these standards to the airline environment became the core focus of this work, ultimately proposing a framework adaptation that has been subject to validation.

The whole project has been built upon logical elements that will now be revisited and finally answered. The initial problem statement launched the development of a number of research questions and global project objectives, for whose achievement a specific project approach has been designed and implemented.

Figure 125: Problem statement and project framework



After all work has been finalised, what can be said about those elements and have the initial research questions been completely answered? This chapter will discuss all results achieved. For this purpose it is also relevant to revisit the initial problem statement to round up all the work performed and shed light into potential further avenues for research.

9.1. Revisiting the initial problem statement

The very first chapter outlined what triggered this research project. Anecdotal evidence showed that risk was not being properly managed by airlines individually, neither in a consistent nor widespread manner by the airline industry. If at all performed, risk management was organised in different manners, with sometimes opposing perceptions of risk. Nevertheless, more information needed to be collected, in quantitative and qualitative manners, to draw solid conclusions on current risk management practices. Therefore, the initial problem statement was formulated in a way to allow addressing all these topics and cover a number of additional underlying issues.

Figure 126: Initial problem statement

Verify the convenience and feasibility of introducing a common risk management model in commercial air transport operators and, if affirmative, identify best practices and standards to help them mitigate the different risks they face.

Underlying issues included:

- Is it convenient to introduce a risk management model at airlines?
- Is it feasible to do so?
- Can such a model be common to all airlines?
- Can such a model be made specific to airlines?
- Are there any relevant best practices and standards that can serve as guideline?
- Can these help mitigate risks faced by airlines?

Airlines have plenty industry-neutral and a few industry-specific standards at their disposal, but as proven during the research process only a minority makes consistent use of these tools in order to manage risks. Nevertheless, several cases of industry best practice have been highlighted, showing that some airlines are leading the way in managing risk. It is certainly possible to design an industry-specific model (as IATA has tried), but the acceptance by the airline community has been limited, in some cases due to regulatory and compliance issues, in others due to sheer lack of interest or knowledge. Most refer to own solutions; very few use available standards. As there was no logical reason to propose a radical new standard, this thesis evolved into adapting the ISO 31000 risk management framework to the airline industry. How does this help answering the research questions? This will be covered in detail in the next section.

9.2. Answers to the research questions

As outlined in Figure 7, there were four initial research questions:

1. What is current practice in airline risk management?
2. What processes and resources are used?
3. Are there improvement areas?
4. How should an airline-specific model be?

The designed project approach and applied work steps enabled collecting information to answer these questions and the more specific issues associated to each of them. The below sections will address each research question individually.

9.2.1. Research Question 1: What is the current practice in airline risk management?

Based on all the findings, the most straightforward answer is: airlines have no common or uniform approach to risk management. From the 100 largest airlines, 30 do not report on risk or don't refer to risk in their reports; of the remaining 70, 32 do not refer to any particular method or standard for risk management purposes. There are 28 referring to COSO, although the large majority of these don't associate this standard to actual risk management practices within the airline. Two further airlines quote the Turnbull Guidance report, another document more focussed on internal audit and control, rather than pure risk management. This means that just 8 airlines refer to a specific risk management standard, either ISO 31000:2009, the older AS/NZS 4360:2004 or even two (one of these and COSO), and even within their approaches one can find standard application differences (as it is by default customisable) and more or less transparent reporting practices.

Based on this, the respective sub-questions initially listed in section 1.3 Research questions, "Is comprehensive risk management a common practice at airlines (or even understood and wanted by higher management)?" and "How much of the internal and external environment is really known, managed and controlled by an airlines' management?" can also be answered.

The first part of the first question receives a clear no: comprehensive risk management is not a common practice at airlines, based on what is reported by the largest airline groups. And this was just a sample of 100 airlines, therefore not all commercial air transport operators. The second part of this question, on risk management being understood and wanted by higher management, it is possible to say that in order to be successful any risk

management efforts must receive support and be endorsed by top management, otherwise it will not gain adherence from middle management layers. Several examples can be cited from the interviews conducted. At one airline the simple exchange of CEO's led to the redirection of focus away from risk management. It has been said that risk management can sometimes be viewed as bureaucratic hurdle in day-to-day business, especially as it does not show immediate and palpable results. The culture change required may take several years and the lack of upper management support will undermine the success of any risk management implementation efforts. Therefore, at another airline, the risk management policy is signed by the CEO and made publicly available for widespread dissemination, recognition and support. Other airlines refer to the existence of such a policy, and the responsibility of the board to approve it, but back away from publicly displaying it on their website or annual reports.

As for the second sub-question on how much of the internal and external environment is really known, managed and controlled by an airline, this is more challenging to produce a clear and unambiguous answer. Neither the survey, nor the interviews produced clear input. Survey results showed that 28 out of 70 airlines report only on basic risk elements, the remaining focus on company internal elements or go as far as covering a larger spectrum of risks. But none goes into explaining what they considered as not covered by their risk management approach. It is of course difficult to answer such a question: it is not possible to know what is unknown, so how can one manage that? The initial chapters of this thesis referred to Taleb's black swan metaphor and this is where it kicks back into the airline business and the topic of this thesis. Earlier on, another statement has been quoted by Mr. Kevin Knight and the surprising lack of inclusion of the Icelandic volcano impacts in the risk landscapes of airlines. ISO 31000 should, per his judgement, enable the inclusion of such events, and yet it wasn't. It is debatable why, but the lack of evidence only opens door to speculative reasoning on possible causes.

In any case, what can be said about this second sub-question is that, and despite the availability of risk management standards and guidance material, that by itself does not eliminate risk and/or their impacts. There will always be events that can harm an airline; there will always be uncertainty affecting the achievement of objectives. As quoted from John Adams in the literature review: there is no zero risk life.

9.2.2. Research Question 2: What processes and resources are used?

Since there is no uniform approach to airline risk management, one can say there is also no common set of processes and resources used by airlines. With the little openness showed by airlines to disclose more detailed information, the answer to this question can only be based on anecdotal evidence collected from individual interviews and/or reports found. For example, Singapore Airlines refers to its 5-step Risk Management process that starts with "Identify" (see Figure 73: Singapore Airlines simplified 5-step Risk Management Process 2011), but little is said about how the actual identification takes place. TAP Portugal shows a 6-steped approach starting with "Identification and Systematisation of Risks" (see Figure 75: TAP Portugal Risk Management process 2009), but their report is also vague when it comes to specifying how this identification is made. The approach presented by Qantas seemed to be the most solid and integrated with other elements of the airline, yet even these are not detailed in content and purpose.

The specialised training events attended for the purpose of this research referred to the possibility of using risk workshops to gather input from several areas of the airline, based for example on stakeholder analysis, SWOT, PESTEL, or other techniques. The IATA IRM standard suggested a way to prepare such a workshop and what techniques could be used during its execution (see Figure 82: IATA Risk Management Workshop Preparations).

From a more generic and industry-neutral perspective, several tools and techniques are mentioned as useful. Figure 29: Quantitative and qualitative risk evaluation methods, listed a few generic methods for quantitative and qualitative evaluations; Figure 51: Applicability of tools used for risk assessment showed the relevance of various tools and techniques in the risk assessment process. To understand what airlines are really using, this list should be subject to a survey of airline risk management staff in order to get their opinions on usage and effectiveness for their own risk management processes. As mentioned earlier, such a survey requires a consistent contact database of airline risk managers, which does not exist. Airlines contacted were mostly not very keen on disclosing certain elements of their risk management approach.

Three separate sub-questions have been listed in the first chapter of this thesis. It is important to answer each of these, too, even though with little base information available.

The first of these sub-questions was: “What process do airlines apply to identify the risks surrounding its business?” As discussed above, airlines tend not to disclose much information on their processes. When mentioned, it is mostly in vague terms with little or no information on exact process elements. Beyond the use of a particular standard, any in-house developed approach or no references to any particular process or standard, not much can be said. A proper answer, that is valid for the industry and not just one airline, can therefore not be given.

The second sub-question was: “How do airlines identify, distinguish and manage risks that are common to the industry and those that are unique to its own business?” The previous paragraphs showed how airlines are (or are not) performing risk identification exercises at their own individual level. On an industry-level little can be said on how common risks are identified or managed. As mentioned in earlier chapters, there is an IATA Working Group on Risk Management whose activities are unknown. The interview with IATA’s Director Risk Management and Insurance showed the difficulties this industry association has in communicating risk related issues with its members. The Association of European Airlines considered risk a commercially sensitive issue, thus it does not have a risk management unit within its own organisation. At Star Alliance level, risk is also considered a sensitive matter, therefore little or no discussions are generated at alliance level. Despite all this, some airline representatives stated that they have discussions with other companies – airlines or not – on risks and other issues, notably comparing processes and improvement potentials. Little information was disclosed on how far these discussions go.

As for the third sub-question “what tools and techniques are available to manage all these risks and are they effective?”, this might be a redundant question as tools and techniques have already been addressed before and effectiveness could not be properly tested. This is probably a field where further research is needed.

9.2.3. Research Question 3: Are there improvement areas?

Yes, most certainly. When risk is not understood and there is little or no risk management as widespread practice in the airline industry – despite the availability of industry-specific risk management standards – something must be done to improve status quo. That the IATA IRM has received little acceptance is visible not only by the survey conducted to the Top 100 airline groups (none mentioned it in their reporting), but also from the statement by IATA that it is difficult to pass on the message on the importance of risk management.

So why do airlines do so little or why are they not so interested? This is another question that truly cannot be answered without using anecdotal evidence. Section 6.1.1 “Limited use of risk management” exposed a number of potential reasons that ranged from lacking guidance to sheer lack of interest. Having an industry-specific standard (as IATA’s) seems not to be enough to convince airlines to apply risk management, although more airlines are introducing related activities (see the case of SATA mentioned earlier).

Given that ISO 31000 is the most recent, most international accepted and already used risk management standard by a few airlines, the thesis evolved into proposing an adaptation of the ISO 31000 risk management framework to allow for easier understanding of concepts and implementation by airlines.

Such an adaptation should be easy to understand, holistic and integrating, aligned with an airlines strategic planning process, enable the involvement of all stakeholders and equip all management layers with tools to manage risk. If well implemented, such an approach should help introducing risk management along the entire airline value chain – from where risk management is still mostly absent.

What about the sub-questions listed as part of this research question; how can they be answered? The following are brief replies to each:

- “Is there a common industry-wide approach or is each airline following its own process?”
  There is no common industry approach, as seen before; every airline tends to adopt the standard it feels most comfortable with or develops its own way.
- “Are “what if” scenarios and “what to do when” portfolios realistic for smaller scale airlines?”
  Certainly, although only integrated into a more robust risk management approach and never as stand-alone exercises. Relying purely on these scenarios may give the perception that the company is covered for all events, which is a great way to fail any risk management effort.
- “How do insurance companies understand risk management at airlines and can they play a bigger role in the risk management process?”
  Interviews conducted to several airline insurance specialists did not provide sufficient material to answer this question properly. Nevertheless the interviewees agree that risk management is not equivalent to insuring the business. Insurance might be one part of the risk management strategy but it doesn’t cover all risks. If insurance companies can play a larger role in the risk management process should be subject of another analysis.

9.2.4. Research Question 4: How should an airline-specific model be?

More than a radical new model, this thesis proposes an adaptation of the ISO 31000 risk management framework to the airline industry. The individual steps described in Chapter 7 show how specific industry issues can be included without disrupting the philosophy behind the ISO 31000 standard. In order to have an approach that is aligned with the airlines' strategic planning, the proposed framework adaptation suggests starting the risk management exercise with collecting basic information on the airlines' strategy, market, stakeholders, value and supply chains. Unique to the industry is the compliance element, where airlines have to meet requirements of national and international bodies on operations and maintenance issues.

This adaptation includes the process implementation as suggested by the ISO 31000 standard. To assist in this process a detailed risk landscape should be produced, the internal risk management organisation defined and the controls available and used for each identified risk listed.

To stress the business aspect of the industry (at the end, the airline business is a business like any other), a third step foresees the continuous revision of results achieved, process feedbacks, gap analysis and a thorough cost-benefit analysis to risk mitigation measures under consideration. Ideally this should help building a risk mitigation toolbox (where the aforementioned "what to do when" portfolios can be included).

The fourth and final element of this proposal is about process adjustments required to further customise the model to the specific airline and/or correct gaps identified during the implementation process.

Given the modular way the proposal has been designed, larger and smaller airlines can apply it, regardless of what resources they have available. In any case its base standard is also customisable by default, thus not all elements must be mandatorily applied.

This approach has been subject to a validation process where several airline risk managers and/or airline risk experts have been invited to comment on the proposal effectiveness, usefulness, stakeholder buy-in and suggested timeframe.

While there was a generally positive welcome to the suggestions made, the indicated timeframe has been classified as too short for such an undertaking. Most of the

participants also suggest this framework is most useful for start up airlines, although some may pick up elements for inclusion in their approach.

As for the sub-questions, there were three separate ones listed in Chapter 1.

- "What would be an ideal risk management model for a smaller airline, with fewer resources?"
  Not necessarily ideal, but a possible model could look like as exposed in Chapter 7. This research question was designed when the project approach still included case studies at airlines, where a joint model development was foreseen as core element of the project. As no airline was available to be case study object, the alternative framework adaptation approach and respective validation testing was the only way to proceed. The suggested adaptation was validated by 7 independent personalities, from large and small airlines, different business models and geographical locations. The feedback was mostly positive and welcoming, although – as expected – some areas can be improved.
- "Is there any lesson to be learned from other industries?"
  Yes, for sure. The thesis analysed in detail the risk management approaches of two companies, one in the telecommunications sector and another in the electricity sector, beyond analysing surveys covering a variety of different industries in various geographical areas. Information collected during this step contributed to the design of the framework adaptation presented in Chapter 7. Elements such as risk materiality, risk management integration, stakeholder identification and involvement are all included in that adaptation. Also the surveys produced by a number of different management consulting firms helped gathering pro's and con's of alternative risk management standards, organisational aspects and other issues.
- "Is ISO 31000 applicable to commercial air transport, as latest risk management standard?"
  Yes. The cases of Qantas and South African Airways prove that ISO 31000 can be used at and by airlines. A full section has been dedicated to answering this question – see 6.1.2 "Can ISO 31000 be used by airlines?", followed by 6.1.3 "Reasons to use ISO 31000 as guiding standard" with a vast array of arguments in favour of using this standard as guideline in this project.

– Intentionally left blank –

10. Conclusions and recommendations

The work conducted in this project led to the compilation of significant results that enabled answering all research questions. The previous chapter provided individual answers to each of those questions. What else can be concluded on the work performed? And have the original project objectives been achieved, too? This final chapter will elaborate on the achievement of those objectives, not only highlighting the limitations of the work presented and approach used, but also stressing the actual contributions and suggestions for further research and development in the fields of airline risk management.

10.1. Achievement of project objectives

There were six independent objectives listed at the beginning of this project which, upon completion of all planned work, need to be checked for its achievement. The following addresses each topic separately, based on the list contained in Figure 8: Project objectives:

- **Answer as many research questions as possible.**
  Most of the research questions have been answered, although some of these answers suffered from the lack of more and deeper information. For example, understanding why ISO 31000 is not used more widely would require more time and resources, beyond a true willingness to cooperate by many more airline representatives. Due to the lack of openness by some entities to share more data a radical new approach, not based on interviews or surveys, would be needed to gather missing elements. In any case, answers provided to the aforementioned four research questions and respective sub-questions enable the understanding of current risk management practices at airlines and open potential new areas for investigation.
- **Expand knowledge in the field of enterprise risk management.**
  While risk management is a journey in itself, doing a research project on the subject proved to be a rewarding challenge. Not only from an individual perspective, where more and new concepts could be apprehended, but the sheer exchange of new information and results achieved with interview partners – most of them veteran risk practitioners in the airline industry – proved that research and knowledge exchange can help the industry move forward.
- **Cover existing gaps in industry-specific literature on the subject.**
  As shown in the early chapters of this thesis, industry-specific literature on risk management is limited in quantity and quality. This project helps, despite all its limitations, to shed light into the generic field, its concepts and definitions, explores industry specific practices, and proposes a risk management framework adaptation that aims at helping airlines address their risk management implementation difficulties. By being as close to the industry as possible, this

proposal can hopefully be taken as direct guidance material for immediate implementation. It won't, nevertheless, replace the base documentation from ISO 31000, rather complement that by clarifying concepts and adding tools for implementation purposes.

- **Provide usable input for the airline community.**
  Based on statements made by some interview and validation counterparts, the proposed framework adaptation will serve as guideline and checklist to review and improve internal risk management approaches. Most of the validation counterparts recognized the completeness of the proposed adaptation and suggested this approach would be useful for airlines willing to start implementing risk management within their businesses. The challenge resides now in sharing this knowledge with airlines and creating interest to continue with actual implementation exercises. As referred earlier, only an implementation of this framework adaptation can help identifying gaps and correct missing elements.
- **Propose a model that combines the best of available industry-neutral standards and industry-specific features.**
  More than a new model, the project evolved into proposing an adaptation of an internationally valid and recognised risk management framework. This adaptation has been made specific to the airline industry and validated by several airline risk managers and risk practitioners from a diverse set of airlines (in size, business model and geographical location). This framework adaptation also contained all the information collected from interviews of airline representatives, risk practitioners and industry experts, as well as quantitative information gathered via a survey conducted to the Top 100 airline groups.
- **Launch a wider debate on possible next steps to implement industry-specific risk management practices.**
  The accomplishment of this project and the recognition of its limitations (mentioned throughout the text and consolidated in the next section) will enable the identification of possible next steps in the development of industry-specific materials and therefore move on with the implementation of more risk management projects at airlines around the globe. The dissemination of the results achieved, the debate on the proposed framework adaptation, and its potential implementation will lead to discussions on its gaps and weaknesses and therefore constantly improve the proposal characteristics for more efficiency and effectiveness of the whole risk management process.

Based on this, it is possible to say that objectives have been mostly achieved. More results can always be aimed for, with more time and resources that were not available. The next section will explore further limitations and shortcomings of this project.

10.2. Limitations and shortcomings

No project is ever completed to the full satisfaction of its promoters. The desire of perfection and completeness drives the need to include more areas and cover all aspects of the respective research field. The above mentioned time and resource limitations hampered most of these desires; shortcomings in the selected project approach also influenced the quantity and quality of results achieved. Further critical issues can be mentioned:

- **Too widely defined research field**, leading to a lack of focus on what is pertinent. This may be said, but given the goals of the project only a widely defined scope could address these goals. A limitation in geography, airline business model, company size or sub-sectors would have shown even fewer data sources and more limited cooperation possibilities from airlines.
- **Too many and too ambitious research questions and project objectives**, making it difficult to focus the approach. Given that the aforementioned research questions and project goals are mostly complementary and interdependent, respective answers helped creating a bigger and better picture on how the industry is performing in terms of risk management, what it wants and how the proposed framework adaptation is received.
- **Inadequate project approach**, not allowing for more detailed conclusions. The initially desired approach based on research, model development and implementation case-studies directly at selected airlines could have led to a more pragmatic, hands-on result, but that would also be so specific to their own operating environment that a replication would be difficult. The ultimately chosen approach of framework adaptation followed by validation, results in a broader and less specific proposal that enables easier customisation at each airline.
- **Long duration of individual work packages**, which were too dependent on external contributions, potentially delaying the production of results and leading to conclusions that – when published – are already outdated. While it was true that interviewing and surveying took its time, notably due to counterpart availability, this was the only possible way to gather information. Actually, the chosen approach allowed for constant information exchange with industry representatives and the continuous updating of information collected, also permitting the witnessing of model evolutions within each airline (see the case of Lufthansa) or the industry in general. Therefore such a criticism is easily revoked by the ultimate prosecution of the chosen approach and the achievement of the initially designed research questions and project objectives.
- **Representative character of surveys and interviews.** Once again, the desire for more quantity is not necessarily equivalent to the retention of more quality. Yes, the survey covered *only* the Top 100 airline groups measured by revenue (equivalent to 70% of the revenue generated by the world's air transport industry);

the interviews included *only* 30 individuals from airlines, consulting firms, insurance companies and related business; and yes, the validation process covered input from *only* seven contributors, all current or former airline risk managers and practitioners. Given the broad coverage of these contributors in terms of airlines, respective business models, company sizes and locations, this is already an impressive collection of input upon which significant conclusions could be drawn.

- **The framework adaptation could have been more detailed**, to include more aspects of the business and the industry. As proven during the validation exercise, the adaptation has been mostly well received by the surveyed industry representatives, as it covers all major areas and enables a holistic view of the airline as a business, not just a flying operation. The proposed framework adaptation is also flexible by design, in the sense that each company willing to implement risk management following these guidelines may choose the components it feels necessary, always keeping the guiding ISO 31000 standard in mind. The goal was not to create a strict handbook of implementation rules and regulations, but show a possible way to implement the leading risk management standard within the airline industry.
- **Limited strength of the validation exercise**, potentially impacted by the goodwill of the contributors. Actually no contributor shied away from criticising the whole proposal or individual elements where they felt was necessary. Strong statements were made on what it should cover (see the statements on more focus on operational issues), its usefulness (some say this proposal would only add limited value to the model already in place, despite saying it would be very valuable to newcomers to risk management) or even the suggested timelines. Comments on the representative character of the participants have also been made earlier. Therefore a criticism on the strength of the validation exercise needs to be tempered with care. A potential add-on to the validation would be the actual implementation of a risk management approach at an airline following the proposed approach. This can be considered a field for further research and development.

Therefore, and given what was possible to be done within the scope and timeframe of this project, the selected approach proved to be the most effective in addressing most relevant issues and produce solid conclusions. The above discussion also highlighted further fields of research that can be pursued in either an academic or professional context. More on this will be discussed in the last section of this chapter.

10.3. Contributions and accomplishments

The vast number of limitations and shortcomings discussed above should not overshadow the many positive aspects of this project, in terms of contributions to knowledge and achieved accomplishments. Beyond having attained the initially outlined project objectives, this section highlights those contributions.

In detail:

- The presented work is the **first of its kind** to combine theoretical literature on risk management with a debate on industry-neutral risk management standards, industry-specific standards and empirical information collected on current industry-specific practices. It therefore covers the identified gap in industry-specific risk management literature and provides food for thought for further studies (see next section on "Suggestions for further research and development").
- **Industry-specific input has been directly sourced from airline representatives**, including risk officers and practitioners, from diverse geographical origins and airline business models, via face-to-face or telephone interviews, trainings and conferences attended. In parallel, an extended survey to corporate management and governance reports of the 100 largest airline groups helped understanding the bigger picture on what is being reported on airline risk management practices, notably focussing on standards used, risk management process design, exercise depth and risk organisation. A survey in such depth and breadth to the largest airlines has never been produced and published before. Other surveys set a stronger focus on aviation insurance issues or risk understood only as related to safety in airline operations.
- **The used project approach enabled the identification of gaps and improvement potentials in current airline risk management practices**. By not focussing on individual risks or giving more importance to specific airline departments (e.g. flight operations, finance), a **holistic view could be generated that contributes to looking at company-wide processes** valid for and usable by all functional units.
- **Best practices from other industries have been incorporated** by looking into cases of companies with internationally recognized risk management practices, as well as considering findings from independent global surveys on risk standards' use and effectiveness. Gathering this input helped collect lessons learned and understand different ways of handling risk management processes and organisations.
- **The result is a clear, simple and ready to use risk management framework adaptation proposal** that is based on the most recent and widely accepted industry neutral risk management standard – ISO 31000 – customised to the airline industry. It provides practical guidance on how to implement the ISO 31000 framework at airlines, regardless of their size, business model or location, but is still flexible to accommodate specific requirements and change requests by individual companies. This proposal has been validated by airline risk managers and risk practitioners.

- **The presented proposal innovates by integrating stakeholders into the risk management process**, as well as by suggesting that risk management should be an ever-present activity along the entire airline value chain. Traditional processes keep stakeholders apart from risk management, despite their obvious impact on the airlines' daily business and global performance. It has also been proven that typical airline value chains exclude risk management, even though it has become an essential management function.
- The implementation of risk management practices based upon **this proposal will help the airline achieve its corporate goals and increase the organisations' resilience** to shocks (of internal or external nature). As it is more formal and exhaustive than risk management models currently used by some airlines, it can easily be used as checklist to ensure completeness. Also, as it addresses a range of areas typically not covered (e.g. strategic management, stakeholder analysis, etc.) it helps questioning and therefore streamlining business fundamentals to its essentials.

Based on all above it is believed that this study adds real value to the scientific and airline communities. By no means does this mean that the study is flawless: the previous list of limitations is quite explicit. Also, improvements can always be made and studies can always go deeper and cover wider topics. Therefore, the next section identifies possible ways to continue research in the field of airline risk management and proceed with improving the herein proposed framework adaptation.

10.4. Suggestions for further research and development

As seen throughout this project, airline risk management still seems to be a field where only the most experienced companies dive into. Very few have advanced risk management models in place or publicly report on their practices. While the pursuing of risk management, aiming at the mitigation of risk impacts, should not only involve individual companies but the entire industry, it would be expectable to see industry bodies positioning themselves to help the airlines – and by that help the industry. As outlined earlier several bodies are not active in this field or are not very transparent in their activities. Therefore, the first suggestion is to engage in closer relationship with industry bodies, identify current risk management activities, member requirements, legal boundaries, etc. in order to produce an industry-wide collaboration model where information can be freely exchanged for the benefit of all stakeholders. Some will say that this involves commercially sensitive issues, true, yet more than discussing individual risks, it would be more about conveying the message of the importance of risk management, process aspects and usable standards. The ultimate goal should be to improve resilience against risks which, in some cases, may be uncontrollable if taken on individually.

Another area that could lead to further investigations is the improvement of the quality of the herein presented framework adaptation proposal. This can only be truly judged if it is ever implemented at an airline. Doing so will require airlines willing to serve as implementation case studies, willingness by internal staff to accept a new project, time to implement it (and as mentioned by some risk managers in the interview process, the implementation can take several years if a full culture change towards risk management is aimed at), a variety of resources allocated to the project and of course upper management support to accomplish the implementation. Based on the improvement potentials found during such an endeavour, not only could the framework adaptation proposal be refined and corrected, but perhaps the ISO 31000 standard could be improved, too.

As combination of both suggestions made above, it would also make sense to build an industry-specific risk management network with contacts of risk officers at all airlines, and take this on to build an industry risk register with associated risk landscapes and control mechanisms. Building this would require active collaboration from individual airlines and industry bodies, as well as full disclosure on control variety and effectiveness. This would come to the benefit of the entire industry and would most certainly lead other industries

into producing similar databases. This might perhaps be part of the vision outlined in Section 7.1 “Goals and vision” and Figure 116: Vision of an holistic risk management approach in the airline industry, yet only the sharing of information can guarantee the long term sustainability of the industry and each member airline.

Other examples could be listed, but all would show that risk and risk management are elements of a never ending journey.

List of References

ABA, 2007. *Aviation Risk Management.* Toulouse, AirBusiness Academy.

Accenture, 2013. *Accenture 2013 Global Risk Management Study - Risk Management for an era of greater uncertainty,* London: Accenture.

ACE European Group Ltd, 2012. *ACE European Risk Briefing 2012,* London: ACE European Group Ltd.

Adams, J., 1995. *Risk.* London: Routledge.

Aerosafe, 2012. *Aviation Risk Management - Course Material.* Wellington: Aerosafe.

Air France KLM, 2011. *Registration Document 2011 - including annual financial report,* Paris: Air France KLM.

Air New Zealand, 2010. *Risk Management Policy,* Auckland: Air New Zealand.

Air New Zealand, 2012. *Iinterim Shareholder Review 2012,* Auckland: Air New Zealand.

Airbus, 2012. *Global Market Forecast 2012-2031,* Toulouse: Airbus.

Airline Business, 2005. Airline Risk Management Survey 2005. *Airline Business*, March.

Airline Business, 2007. Airline Risk Management Survey 2007. *Airline Business*, March.

Airline Business, 2012. Airline Business World Airline Rankings 2012. *Airline Business*, August, pp. 44-51.

AIRMIC, ALARM, IRM, 2002. *A Risk Management Standard,* Brussels: FERMA.

AIRMIC, IRM, 2009. Review of the effectiveness of the Combined Code.

AIRMIC, 2005. *An overview comparison of the AIRMIC/ALARM/IRM Risk Management Standard with AS/NZS 4360:2004 and COSO,* London: AIRMIC.

Albers, S., Koch, B. & Ruff, C., 2005. Strategic Alliances between airlines and airports - theoretical assessment and practical evidence. *Journal of Air Transport Management,* 11(2), pp. 49-58.

AON, 2013. *Global Risk Management Survey 2013,* Dublin: AON Risk Solutions.

Association of European Airlines, 2011. *e-mail exchange with AEA's Secretariat requesting for information on risk related activities.* Brussels: s.n.

Battal, Ü., 2008. *Risk Management in Airlines: Financial Risks at Turkish Airlines,* New York: Global Business and Technology Association.

Baxter, K., 2010. *Risk Management.* Harlow: Pearson Education Limited.

Beck, U., 1992. *Risk Society - Towards a New Modernity.* London: Sage Publications Ltd.

Beck, U., 2009. *World at Risk.* Cambridge: Polity Press.

Bedford, T. & Cooke, R., 2001. *Probabilistic Risk Analysis - Foundations and Methods.* Cambridge: Cambridge University Press.

Belobaba, P., Odoni, A. & Barnhart, C., 2009. *The Global Airline Industry.* Chichester: John Wiley & Sons Ltd.

Bernstein, P. L., 1996. *Against the Gods - The remarkable story of risk.* New York: John Wiley & Sons, Inc..

Bernstein, P. L., 2009. *McKinsey & Company.* [Online]
Available at: www.whatmatters.mckinseydigital.com
[Accessed 4 February 2010].

Boeing, 2013. *Current Market Outlook 2013-2032 Presentation,* Chicago: The Boeing Company.

Brodeur, A. & Pritsch, G., 2008. Making risk management a value-adding function in the boardroom. *McKinsey Working Papers on Risk*, Number 2, September.

Buehler, K., Freeman, A. & Hulme, R., 2008. The risk revolution. *McKinsey Working Papers on Risk*, September.

Buehler, K. S. & Pritsch, G., 2003. Running with risk. *McKinsey Quarterly*, November, pp. 40-49.

Cathay Pacific, 2009. *Cathay Pacific Annual Report 2008,* Hong Kong: Cathay Pacific.

Cathay Pacific, 2012. *Corporate Governance Report 2011,* Hong Kong: Cathay Pacific.

Chopra, D. et al., 2009. Responding to the variable annuity crisis. *McKinsey Working Papers on Risk*, Number 10, April.

Chow, N. Y., 2007. *Developing a Methodology in Aviation Risk Management based on Susceptibility,* Kuala Lumpur: University of Sciences Malaysia.

Clark, P., 2010. *Stormy Skies - Airlines in Crisis.* Farnham: Ashagte Publishing Limited.

Clegg, S., 2010. *Risk Management Standards for SMS, High Level Safety Conference 2010.* Montreal, ICAO International Civil Aviation Organisation.

CME Group, Inc., 2010. *Agriculture Products - Wheat Futures.* [Online]
Available at: www.cmegroup.com
[Accessed 8 August 2010].

Coleman, L., 2009. *Risk Strategies - Dialling up optimum firm risk.* Farnham: Gower Publishing Limited.

COSO, 2004. *Enterprise Risk Management - Integrated Framework, Application Techniques.* Jersey City: AICPA.

COSO, 2004. *Entreprise Risk Management - Integrated Framework.* Jersey City: AICPA.

COSO, 2009. *Strengthening Entreprise Risk Management for Strategic Advantage,* s.l.: The Committee of Sponsoring Organisations of the Treadway Commission.

COSO, 2010. *Developing Key Risk Indicators to Strengthen Enterprise Risk Management,* Durham: COSO.

Deloitte, 2013. *Global risk management survey, 8th edition - Setting a higher bar,* London: Deloitte Touche Tohmatsu Limited.

Deloitte, Hwang, S. & Peretz, A., 2010. *A new global standard for risk management - Inside ISO 31000:2009,* Toronto: Deloitte.

DJSI - RobecoSAM, 2013. *Industry Group Leader Report - EDP Energias de Portugal ,* Zürich: DJSI - RobecoSAM.

Doganis, R., 2002. *Flying Off Course.* 3 ed. London: Routledge.

Douglas, M. & Wildavsky, A., 1992. *Risk and Culture.* Los Angeles: University of California Press.

EDP Energias de Portugal, 2012. *Annual Report 2012,* 2013: EDP Energias de Portugal.

EDP Energias de Portugal, 2013a. *Corporate Business Risk Management Policy.* [Online]
Available at: http://www.edp.pt/en/aedp/sobreaedp/principiosepoliticas/Pages/politica-gestao_empresarial_risco.aspx
[Accessed 18 October 2013].

EDP Energias de Portugal, 2013b. *EDP Energias de Portugal - About EDP - Strategy.* [Online]
Available at: www.edp.pt
[Accessed 13 October 2013].

EDP Energias de Portugal, 2013c. *EDP Energias de Portugal - Recognition.* [Online]
Available at:
http://www.edp.pt/en/sustentabilidade/abordagemasustentabilidade/premios/Pages/Premios2.aspx
[Accessed 18 October 2013].

EDP Energias de Portugal, 2013d. *Sustainable Development - May 2013,* Lisboa: EDP Energias de Portugal.

Ernst & Young, 2009. *The 2009 Ernst & Young business risk report,* London: Ernst & Young.

Ernst & Young, 2010. *The Ernst & Young Business Risk Report 2010,* London: Ernst & Young.

Ernst & Young, 2012. *Turn risks and opportunities into results,* London: Ernst & Young.

Ernst & Young, 2013. *Turn risks and opportunities into results,* London: Ernst & Young.

EURELECTRIC, 2014. *EURELECTRIC - Electricity for Europe - About Us.* [Online]
Available at: http://www.eurelectric.org/about-us/
[Acedido em 30 January 2014].

European Corporate Governance Institute, 2013. *European Corporate Governance Institute.* [Online]
Available at: www.ecgi.org
[Accessed 5 July 2013].

European Interagency Security Forum, 2010. *Risk Management Standards - Summary and Comparison.* [Online]
Available at: www.eisf.eu
[Accessed 5 July 2013].

European Parliament and European Council, 2006. *DIRECTIVE 2006/43/EC on statutory audits of annual accounts and consolidated accounts, amending Council Directives,* Brussels: European Parliament and European Council.

FEDEX, 2011. *Annual Report 2011,* Memphis: FEDEX.

FERMA, ECIIA, 2010. *Guidance on the 8th EU Company Law Directive - article 41,* Brussels: FERMA, ECIIA.

FERMA, 2006. *Risk Management Practices in 2006: Are you ready for change ?,* Brussels: FERMA Federation of European Risk Management Associations.

FERMA, 2008. *FERMA European risk management benchmarking survey 2008,* Brussels: FERMA Federation of European Risk Management Associations.

FERMA, 2010. *FERMA risk management benchmarking survey 2010,* Brussels: FERMA Federation of European Risk Management Associations.

FERMA, 2012. *FERMA European Risk Management Benchmarking Survey 2012,* Brussels: FERMA Federation of European Risk Management Associations.

Fernando, S., 2006. *Risk Management Practices in the Airline Industry,* Burnaby: Simon Fraser University.

Finnair, 2011. *Annual Report 2011,* Helsinki: Finnair.

Finnair, 2013. *Financial Report 2012,* Helsinki: Finnair.

Flightglobal, 2012. *Organisational resiliance 'key to coping with risks to reputation'.* [Online]
Available at: www.flightglobal.com
[Accessed 13 September 2013].

FRC, 2005. *Internal Control: Revised Guidance for Directors on the Combined Code,* London: Financial Reporting Council.

FRC, 2011. *Boards and Risk: A summary of discussions with companies, investors and advisers,* London: Financial Reporting Council.

G31000 Global Risk Management Platform, 2012. *Global ISO 31000 Survey 2011.* Paris, G31000 Global Risk Management Platform.

Garuda Indonesia, 2012. *Annual Report 2011,* Jakarta: Garuda Indonesia.

Giddens, A., 1990. *The Consequences of Modernity.* Cambridge: Polity Press.

Gittel, J. H., Cameron, K., Lim, S. & Rivas, V., 2006. Relationships, Layoffs and Organisational Resilience: Airline Industry Responses to September 11. *The Journal of Applied Behavioural Science,* 42(3), pp. 300-329.

Government of South Australia, Department of Health, March, 2006. *Risk Management - Policy and Framework,* Adelaide: Government of South Australia, Department of Health.

Harrington, S. E. & Niehaus, G. R., 2003. *Risk Management & Insurance.* New York: McGraw-Hill Companies, Inc..

Harvard Business Review, 2013. *Leadership in Risk Management,* Boston: Harvard Business Review Analytic Services.

Hillson, D. & Murray-Webster, R., 2007. *Understanding and Managing Risk Attitude.* 2nd ed. Aldershot: Gower Publishing Limited.

HM Treasury, 2004. *The Orange Book - Management of Risk - Principles and Concepts.* London: HM Treasury.

Hubbard, D. W., 2009. *The Failure of Risk Management - Why it's broken and how to fix it.* New Jersey: John Wiley & Sons, Inc.

IAG Group, 2012. *Annual Report and Accounts 2011,* London: IAG Group.

IATA, 2009. *Airlines International, December 2009.* [Online]
Available at: http://www.iata.org/publications/airlines-international/december-2009/Pages/03.aspx
[Accessed 18 July 2013].

IATA, 2010. *Integrated Risk Management Guidance Manual.* Montreal: IATA International Air Transport Association.

IATA, 2012a. *Annual Review 2012,* Geneva: IATA International Air Transport Association.

IATA, 2012b. CEO Interview - Icelandair. *Airlines International*, October.

IATA, 2012c. Special Report - Risk Management Strategies - Read the Small Print. *Airlines International*, December.

IATA, 2013a. *IATA - Fuel Price Analysis.* [Online]
Available at: http://www.iata.org/publications/economics/fuel-monitor/Pages/price-development.aspx
[Accessed 9 February 2013].

IATA, 2013b. *Foundations of Risk Management.* Singapore, IATA International Air Transport Association.

IATA, 2013c. *IATA Standards & Manuals.* [Online]
Available at: www.iata.org
[Accessed 14 July 2013].

IATA, 2013d. *Profitability and the air transport value chain - IATA Economics Briefinf nº10,* Geneva: IATA International Air Transport Association.

Iberia, 2010. *Iberia Group Consolidated Management Report / Annual Corporate Governance Report 2009,* Madrid: Iberia.

ICAO, 2009. *Safety Management Manual - Doc 9859 AN/474,* Montreal: ICAO International Civil Aviation Organisation.

ICAO, 2010. *The ARMS Methodology for Operational Risk Assessment in Aviation Organisations,* Montreal: ICAO International Civil Aviation Organisation.

IMA, 2007. *Enterprise Risk Management: tools and techniques for effective implementation,* Montvale, New Jersey: Institute of Management Accountants.

Immameni, A., Mastro, C. & Haubenstock, M., 2004. A Structured Approach to Building Predictive Key Risk Indicators. *Operational Risk: A Special Edition of The RMA Journal*, Month, pp. 42-47.

Institute of Directors in Southern Africa, 2009. *King Report,* Johannesburg: Institute of Directors in Southern Africa.

Institute of Internal Auditors, 2013. *IIA Position Paper: The three lines of defense in effective risk manafement and control,* Altamonte Springs, Florida: Institute of Internal Auditors.

Institute of Operational Risk, 2010. *Key Risk Indicators,* Ware: Institute of Operational Risk.

International Organisation for Standardisation, 2009a. *ISO/FDIS 31000:2009 Risk Management - Principles and guidelines.* Geneva: ISO.

International Organisation for Standardisation, 2009b. *IEC/FDIS 31010:2009 Risk Management - Risk Assessment Techniques.* Geneva: International Organisation for Standardisation.

International Organisation for Standardisation, 2009c. *Guide 73 Risk Management - Vocabulary - Guidelines for use in standards.* Geneva: International Organisation for Standardisation.

ISACA, 2010. *Risk Management Discussion.* [Online]
Available at: http://www.isaca.org/Groups/Professional-English/risk-management/Pages/ViewDiscussion.aspx?PostID=26
[Accessed 21 January 2014].

Japan Airlines, 2010. *Annual Report 2009,* Tokyo: Japan Airlines.

Jenner, G., 2006. Risk Profile. *Airline Business*, May, pp. 62-65.

Jenner, G., 2007. Premium Rate. *Airline Business*, June, pp. 74-76.

Jones, M., 2013. *Strategic Risk Magazine.* [Online]
Available at: www.strategic-risk-global.com
[Accessed 19 December 2013].

Knight, K. W., 2009a. *Transitioning to the new risk management standard.* Canberra, Comcover - Australian Government, Department of Finance and Deregulation.

Knight, K. W., 2009b. *New ISO standard for effective management of risk.* [Online]
Available at: www.iso.org
[Accessed 9 August 2010].

Knight, K. W., 2010. *ISO 31000 and the Icelandic volcano crisis.* [Online]
Available at: www.iso.org
[Accessed 9 August 2010].

Knight, K. W., 2011. *Risk Management - New work reinforces a solid toolbox.* [Online]
Available at: www.iso.org
[Accessed 10 September 2012].

KPI Library - ServiceNow, 2014. *KPI Library.* [Online]
Available at: www.kpilibrary.com
[Accessed 21 January 2014].

KPMG, 2013. *Expectations of Risk Management Outpacing Capabilities - It's time for Action,* Houston: KPMG International.

Lamarre, E. & Pergler, M., 2009. Risk: seeing around the corners. *McKinsey Quarterly*, October.

Lam, J., 2007. *Operational Risk Management - beyond compliance to value creation,* Waltham: www.openpages.com.

Lam, J., January 2007. *Entreprise Risk Management at Asian Banks: from Challenges to Strategies,* Singapore: Asia Risk Management Institute.

Lam, J., September 2006. *Emerging best practices in developing key risk indicators and ERM reporting,* s.l.: Jason Lam & Associates.

Laubsch, A. J. & Ulmer, A., 1999. *Risk Management: a practical guide,* s.l.: RiskMetrics Group, LLC.

Loudon, G. F., 2004. Financial risk exposures in the airline industry: evidence from Australia and New Zealand. *Australian Journal of Management,* 29(2, December), pp. 295-316.

Lovallo, D. P. & Sibony, O., 2006. Distortions and deceptions in strategic decisions. *The McKinsey Quarterly,* Issue 1, pp. 19-29.

Lufthansa German Airlines , 2013. *Annual Report 2012,* Frankfurt: Lufthansa German Airlines.

Lufthansa German Airlines, 2004. *Annual Report 2003,* Frankfurt: Lufthansa German Airlines.

Lufthansa German Airlines, 2008. *Annual Report 2007,* Frankfurt: Lufthansa German Airlines.

Lufthansa German Airlines, 2012. *Annual Report 2011,* Frankfurt: Lufthansa.

Lufthansa German Airlines, 2013. *Corporate Governance.* [Online]
Available at: http://investor-relations.lufthansa.com/en/corporate-governance.html
[Accessed 9 February 2013].

Marks, N., 2012. *Norman Marks on Governance, Risk Management and Audit.* [Online]
Available at: http://normanmarks.wordpress.com/2012/05/11/final-results-of-coso-vs-iso-risk-management-survey/
[Accessed 30 August 2013].

Marsh, 2013. *Delivering Strategic Value through Risk Management,* New York: Marsh&McLennan.

Miller, T., 2010. *PBS News.* [Online]
Available at: www.pbs.org
[Accessed 10 August 2010].

Nomura, K., 2003. Managing Risks in Airline Industry. *Japan and the World Economy,* 15(4), pp. 469-479.

Oliver Wyman, 2005. *What's your risk appetite? - How much risk do you want to take?,* New York: Oliver Wyman.

Oliver Wyman, 2012. *The Oliver Wyman Risk Journal,* London: Oliver Wyman.

Pandor, I., Thomas, L. & Schüller, J., 2010. *Risk appetite: a key management tool (Insurance Countdown, July 2010),* London: PriceWaterhouseCoopers.

Pellerin, M., Smith-Bingham, R. & Wittenberg, A., 2012. Managing a company's risk appetite effectively can be the difference between long-term sucess and failure. *Risk Journal - Oliver Wyman*, June, pp. 15-19.

Pergler, M. & Freeman, A., September, 2008. Probabilistic modelling as an exploratory decision-making tool. *McKinsey Working Papers on Risk,* Issue 6.

Portugal Telecom, 2013a. *Corporate Governance Report 2012,* Lisboa: Portugal Telecom.

Portugal Telecom, 2013b. *Annual Report 2012,* Lisboa: Portugal Telecom.

Portugal Telecom, 2013c. *Corporate Sustainability Report 2012,* Lisboa: Portugal Telecom.

Power, M., 2007. *Organised Uncertainty - Designing a world of risk management.* Oxford: Oxford University Press.

PriceWaterhouseCoopers, 2010. *Risk appetite: a key management tool,* London: PriceWaterhouseCoopers.

Pritsch, G., Stegemann, U. & Freeman, A., 2008. Turning risk management into a true competitive advantage. *McKinsey Working Papers on Risk,* Issue 5, September.

Protiviti, 2012. *Defining Risk Appetite,* New York: Protiviti.

Purdy, G., 2009. *Raising the standard - the new ISO Risk Management Standard.* Wellington, Society for Risk Analysis.

Qantas, 2010. *Qantas Group Constitution,* Sydney: Qantas.

Qantas, 2011a. *Annual Report 2011,* Sydney: Qantas.

Qantas, 2011b. *Audit Committee Charter,* Sydney: Qantas.

Qantas, 2011c. *Qantas Group Data Book,* Sydney: Qantas.

Qantas, 2012a. *Qantas Group Business Practices Document,* Sydney: Qantas.

Qantas, 2012b. *Qantas Group Risk Assessment Guide,* Sydney: Qantas.

Rapajic, J., 2009. *Beyond Airline Disruptions.* Farnham: Ashgate Publishing Limited.

Raz, T. & Hillson, D., 2005. A Comparative Review of Risk Management Standards. *Risk Management: An International Journal,* 7(4), pp. 53-66.

Reason, J., 1997. *Managing the Risks of Organisational Accidents.* Aldershot: Ashgate Publishing Ltd.

RIMS, 2011. *RIMS Executive Report - An overview of widely used risk management standards and guidelines,* New York: RIMS.

Sadgrove, K., 2005. *The Complete Guide to Business Risk Management.* Aldershot: Gower Publishing Limited.

Salter, M. B., 2008. Imaginig numbers: risk, quantification and aviation security. *Security Dialogue,* 39(2-3, April), pp. 243-266.

Securities and Exchange Commission, 2007. *Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934,* Washington: Securities and Exchange Commission.

Senate and House of Representatives of the United States of America, 2002. *Sarbanes-Oxley Act of 2002, Public Law 107-204,* Washington: Senate and House of Representatives of the United States of America.

Singapore Airlines, 2009. *Singapore Airlines Annual Report 2008-2009,* Singapore: Singapore Airlines .

Singapore Airlines, 2012. *Annual Report 2011/2012,* Singapore: Singapore Airlines.

Standards Australia / Standards New Zealand, 1999. *AS/NZS 4360:1999 Risk Management.* Strathfield: Standards Association of Australia.

Standards Australia / Standards New Zealand, 2004. *AS/NZS 4360:2004 Risk Management.* Strathfield: Standards Association of Australia.

Standards Australia / Standards New Zealand, 2013. *Draft for Public Comment: Australian/New Zealand Hanbook - Risk Management Guidelines Companion to AS/NZS ISO 31000:2009; Committee OB-007 - Risk Management,* Sydney / Wellington: Standards Australia / Standards New Zealand.

Stulz, R. M., 2009. Six Ways Companies Mismanage Risk. *Harvard Business Review*, March.

Taleb, N. N., 2007. *The Black Swan.* London: Penguin Books Ltd.

TAP Portugal, 2010. *Corporate Governance and Sustainability Report 2009,* Lisbon: TAP Portugal.

TAP Portugal, 2012. *Corporate Governance and Sustainability Report 2011,* Lisbon: TAP Portugal.

The Economist Intelligence Unit, 2007. *Best practice in risk management - a function comes of age,* London: The Economist Intelligence Unit Limited.

The Economist Intelligence Unit, 2009. *Managing risk in perilous times - practical steps to accelerate recovery,* London: The Economist Intelligence Unit Limited.

The Economist, 2007. Fear of flying - A special report on air travel. *The Economist*, 16 June.

The Economist, 2010. The gods strike back - a special report on financial risk. *The Economist*, 13 February.

The Institute of Internal Auditors, 2010. *The New International Standard on the Practice of Risk Management – A Comparison of ISO 31000:2009 and the COSO ERM Framework,* Altamonte Springs: The IIA.

TUI Travel, 2013. *Annual Report & Accounts 2012,* London: TUI Travel PLC.

UBM Aviation, 2011. *World Crisis Analysis,* London: UBM Aviation - OAG Market Intelligence.

Walker, S., February 2009. *Enterprise Risk Management: The Art of Avoiding Unpleasant Surprises,* Boston: Aberdeen Group Inc..

Weiss, D. & Maher, M. W., 2009. Operational hedging against adverse circumstances. *Journal of Operations Management,* Issue 27, pp. 362-373.

Wells, A. T. & Chadbourne, B. D., 2007. *Introduction to Aviation Insurance and Risk Management.* 3rd ed. Malabar, Florida: Krieger Publishing Company.

World Economic Forum, 2012. *Global Risks 2012,* Geneva: World Economic Forum.

World Economic Forum, 2013a. *Global Risks 2013,* Geneva: World Economic Forum.

World Economic Forum, 2013b. *Building Resilience in Supply Chains,* Geneva: World Economic Forum.

Yilmaz, A. K., 2008. *The best Enterprise Risk Management pratice for airline and airport business.* Saarbrücken: VDM Verlag Dr. Müller Aktiengesellschaft & Co. KG.

Yilmaz, A. K. & Flouris, T., 2010a. *Strategic Management in the Airline Business: the entreprise sustainability risk management conceptual model.* Lisbon, WCTR - World Conference on Transport Research Society.

Yilmaz, A. K. & Flouris, T., 2010b. *The management of reputation risk and airline sustainability.* Lisbon, WCTR - World Conference on Transport Research Society.

Yilmaz, A. K. & Kucuk, F., 2010. The Reputation Crisis: Risk Management based Logical Framework to the Corporate Sustainability. In: M. Pomffyova, ed. *Process Management.* s.l.:InTech, pp. 223-244.

Zea, M., 2002. Is airline risk manageable?. *Airline Business*, April.

Zech, J., 2001. Rethinking risk management: the combination of financial and industrial risk. *The Geneva Papers on risk and insurance,* 26(1), pp. 71-82.

Annexes

A. Interview template

The below template has been used for the face-to-face, telephone and e-mail interviews conducted during the research process. The results of these interviews have been summarized in section "5.3 Summary of interviews conducted". As per interviewees request, their respective answers have been kept anonymous.

Meeting/Interview Note #XYZ

Interviewee:

Organisation:
Position:

Location, Date:
Duration (approx):

Note: please feel free to use the boxes below for your comments and answers.

Context	
1.	When and in what context did your airline introduce the Entreprise Risk function?
	Your answer here...
2.	How was risk managed before the introduction of this function?
	Your answer here...
3.	How much time was invested from beginning (structure design, function definition, team gathering, project implementation, etc.) until the actual start of the unit's work?
	Your answer here...
4.	How did the Entreprise Risk function contribute to the improved management of risk at your airline? Was the success of the function (immediately) visible and/or measurable?
	Your answer here...

Process & Organisation	
5.	What process has been implemented, how does it work and what are its key elements?
	Your answer here...
6.	Does your airlines' model foresee a centralized risk management function for all business units within the company or was it a decentralized model where each unit was responsible for managing its own risks?
	Your answer here...
7.	Did your airline gather inspiration and input from other risk management models

	already implemented at other airlines or industries? If yes, which ones and why?
	Your answer here...
8.	How many people are directly involved in the risk management process? Do these people have a skill-set that makes them more suitable for the job? Is communication among them easy and fluid?
	Your answer here...
9.	What problems occurred during and after the implementation of the model? How well was it accepted by the direct and indirect users, has it ever been seen as another bureaucratic step?
	Your answer here...
10.	How does the model integrate operational and non-operational risks?
	Your answer here...
11.	Did your airline follow any risk management standard available at that time and/or has your airlines' approach to risk management been updated or changed since its implementation (COSO, ISO 31000, etc)?
	Your answer here...
12.	How (and when) do you know the process worked?
	Your answer here...
13.	To whom do you as Head of Risk Management report to? How far away are you from top management and do you have a direct reporting line to the board of directors or other units with your airline, too?
	Your answer here...
14.	Some companies have combined risk management and internal audit functions. Were these kept separate at your airline; if yes, why?
	Your answer here...

Risk Management	
15.	At your airline, what is considered a risk? Is there an airline-internal common definition of risk, and respective harmonized risk language?
	Your answer here...
16.	How does your airline identify risks? How fast is acted upon? What are the steps in the process to manage each risk? Can you give examples?
	Your answer here...
17.	How does your airline handle risks that were not manageable (or insurable), notably the ones that are beyond your airlines' control?
	Your answer here...
18.	How does your airline proceed with unidentifiable risks (unknown unknowns)?
	Your answer here...
19.	In the risk management process, does your airline cooperate with other airlines and/or industry bodies (IATA, AEA, UK CAA, Eurocontrol) in order to manage risks that were common to the industry? Can you give examples?
	Your answer here...
Policy and management	

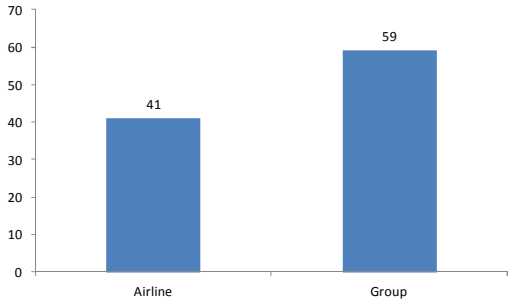
20.	From a management perspective, what level of detail is reported to upper management?
	Your answer here...
21.	How would you define the risk appetite at your airline? Do you think it changed since you have left the company?
	Your answer here...
22.	Does your airline have a risk policy that is publicly communicated? As example, Air New Zealand publishes its Risk Policy online on their website (http://www.airnewzealand.co.nz/corporate-governance-policies).
	Your answer here...

Other topics	
23.	
	Your answer here...
24.	
	Your answer here...

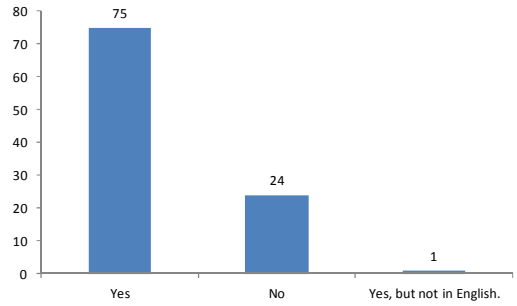
B. Survey results summary

The below summarizes the findings of the survey conducted to the Annual Reports, Corporate Governance Reports and Social Responsibility Reports of the Top 100 Airline Groups, measured by revenue, as ranked by the Airline Business Magazine in its August 2012 edition. A complete analysis of this survey and respective results is included in section "5.2 Top 100 airlines survey results".

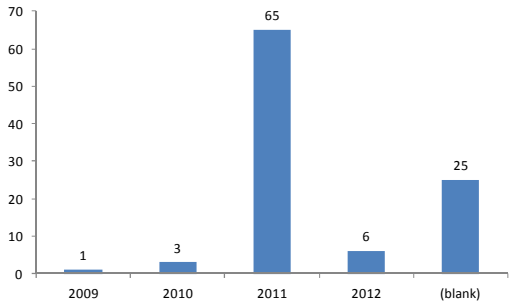
Q1: Is this one airline or a group of airlines?



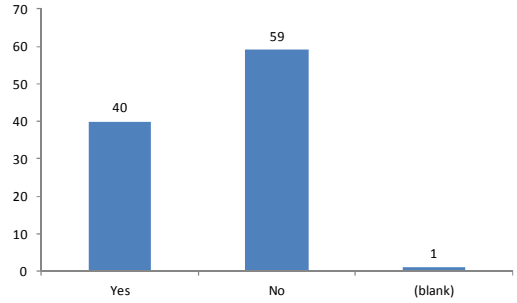
Q2: Does the airline/group publish an Annual Report?



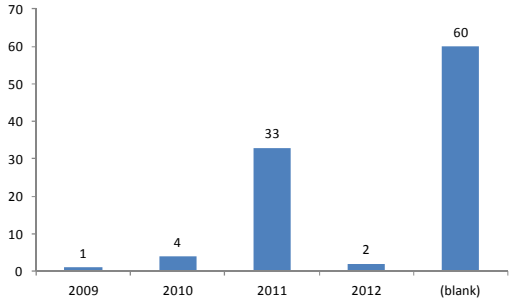
Q3: The latest available refers to what year?



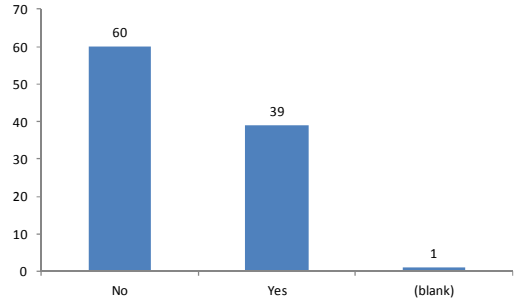
Q4: Does the airline/group publish a Social Responsibility report?



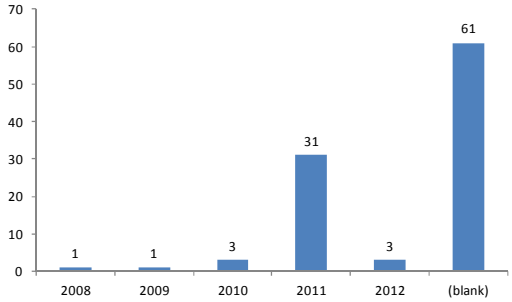
Q5: The latest available refers to what year?



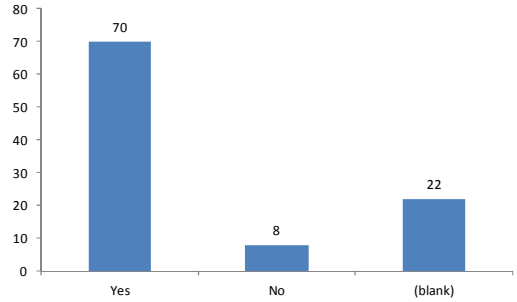
Q6: Does the airline/group publish a Corporate Governance report?



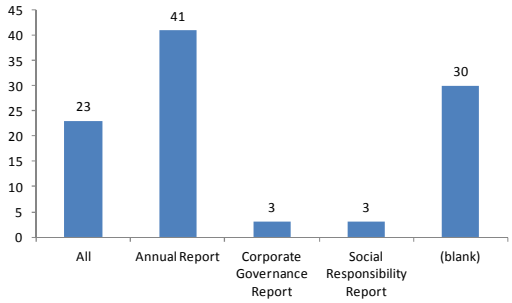
Q7: The latest available refers to what year?



Q8: Is Risk Management mentioned in any of these reports?



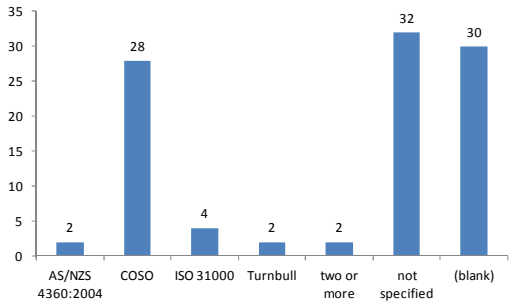
Q9: Where?



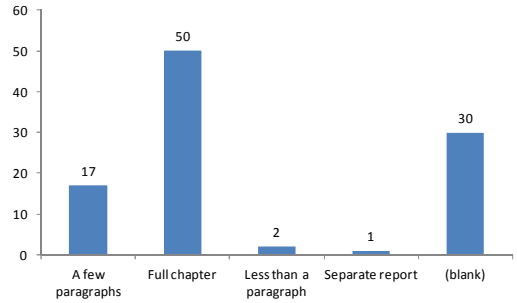
Q10: How is Risk defined?
(free text answer)

- "Not defined"… large majority of cases
- "Events that could potentially affect the Group and prevent it from achieving its objectives", AirFrance-KLM
- "Risks count as material if they are capable of causing damage of at least one third of the operating result necessary for maintaining the value of the Company. For 2011 this amount was again determined to be EUR 300m for the Lufthansa Group", Lufthansa Group

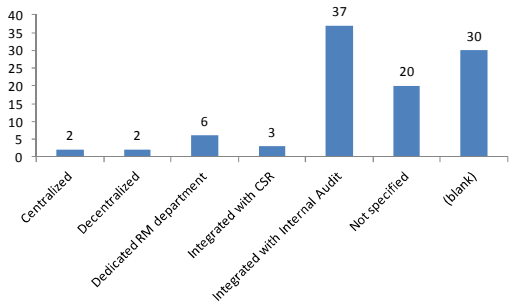
Q11: What standard is mentioned?



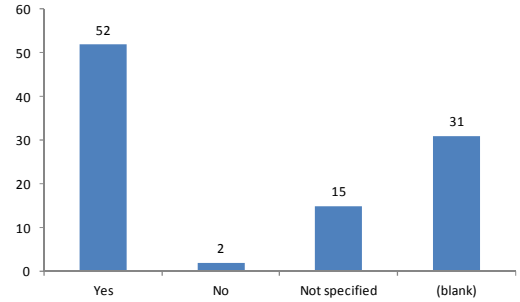
Q12: How much volume is dedicated to RM in that report?



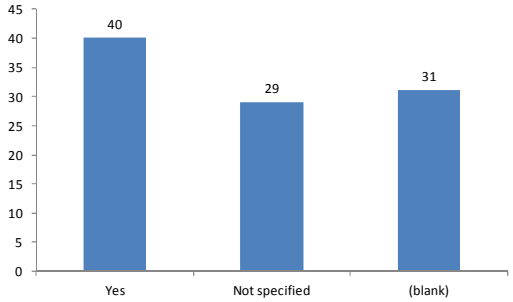
Q13: What RM organization is visible from that report?



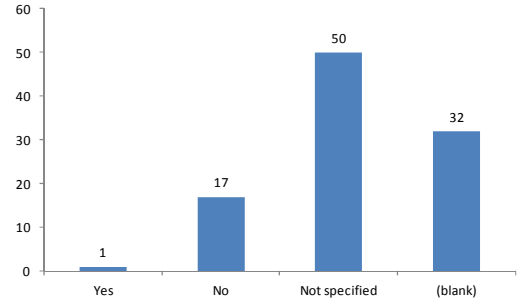
Q14: Is RM integrated into its Corporate Governance model?



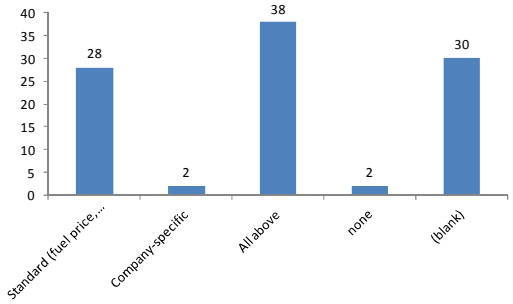
Q15: Does this RM approach cover all airlines in the group?



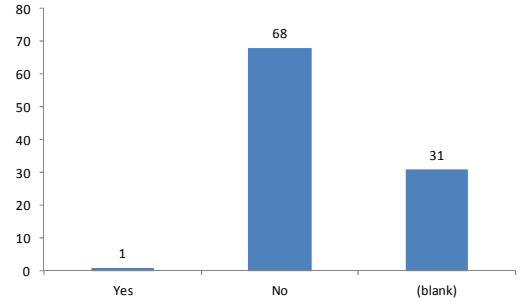
Q16: Do other airlines in the group have different approaches to RM?



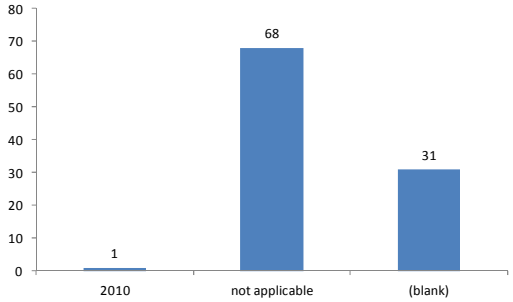
Q17: What risks are mentioned in the above reports?



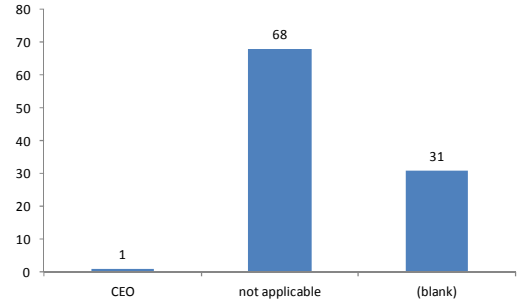
Q18: Does the group have a publicly available Risk Management policy?



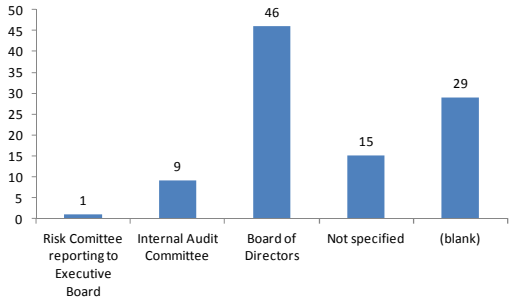
Q19: When was this last updated?



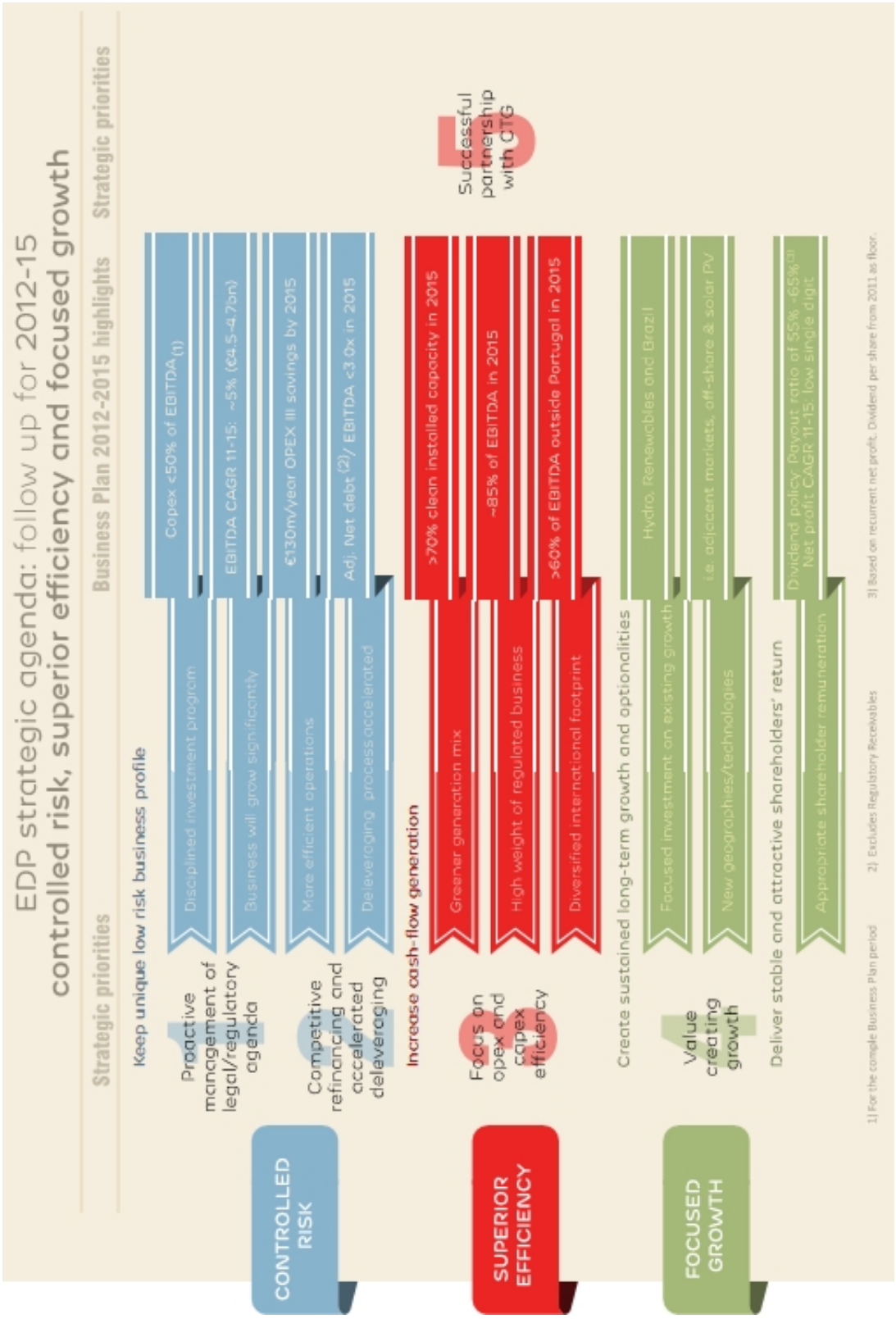
Q20: Who signed this RM policy?



Q21: How is Risk discussed and managed?



C. EDP Strategic Agenda 2012-2015



D. Risk Management Framework Presentation

The below copied presentation summarizes the risk management framework adaptation proposal that has been sent to a select group of airline risk management experts in the context of the validation process as outlined in chapter “8. Proposal validation”. These experts have been invited to answer four questions:

1. “How would the proposed framework enable your airline to achieve a more effective risk management process? If not, why?”
2. “Would you consider using elements of the framework (in full or just some elements) to improve the risk management process at your airline? If yes, which elements; if no, why? Or would you consider this framework to be more useful for airlines just about to start their risk management efforts?”
3. “Is it realistic to aim at getting the buy-in of all stakeholders in the risk management process, so that the entire industry becomes more risk aware, or is this an unachievable goal? Please elaborate.”
4. “Do you think it is possible to implement a risk management process based on such a framework within the proposed timeframe (6-9 months, depending on airline size and complexity) or does any element need to be adjusted?”

All answers are included in the aforementioned chapter of the main document.

PhD: Holistic Risk Management in Commercial Air Transport
Airline Risk Management Framework
by Paulo Nunes

Lisbon, 22nd August 2013

CITY UNIVERSITY LONDON | School of Engineering

Contents

Improving an organisations' resilience over time and to unforeseen events is a challenge

Key Questions:

1. What goals and objectives does your organisation want to achieve?
2. What can affect the achievement of those objectives?
3. How is your organisation addressing these issues?
4. How effective are these control measures?
5. How resilient is your organisation?

Aligning resources to enable the achievement of objectives is a simple definition of risk management

Definition of risk :

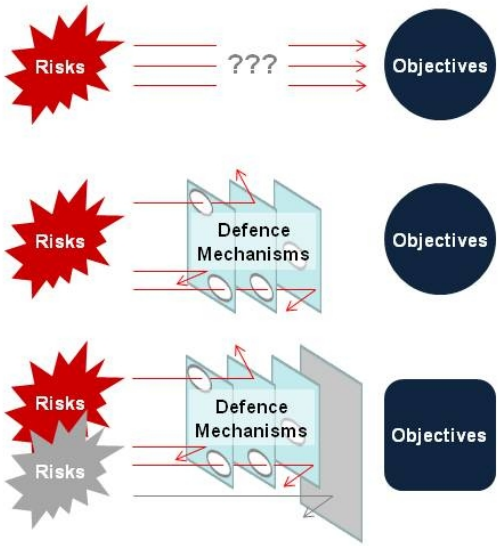
"Effect of uncertainty on objectives"

Definition of risk management:

"Coordinated activities to direct and control an organization with regard to risk"

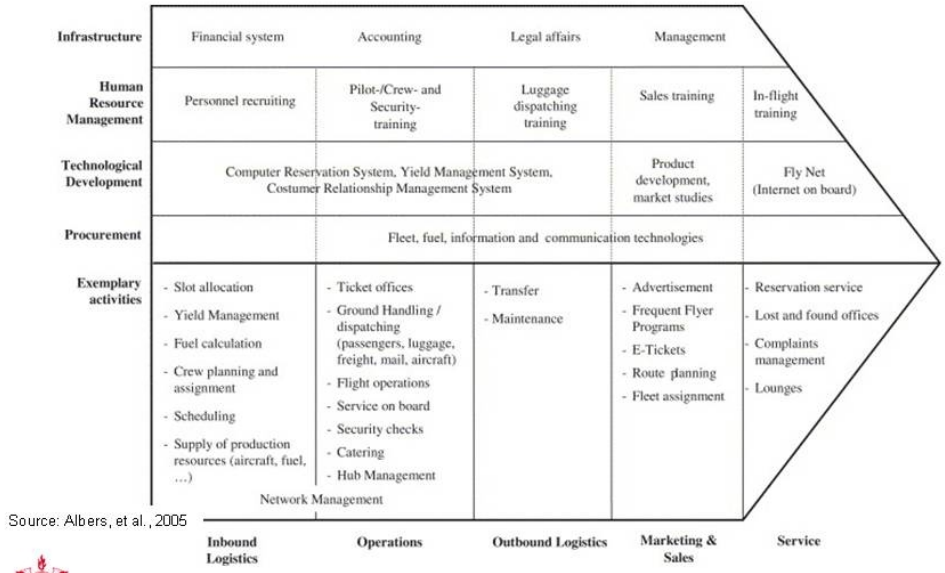
Definition of resilience:

"Adaptive capacity of an organization in a complex and changing environment "



Source: ISO31000 / Guide73

Traditional airline value chains do not include any formalised risk management

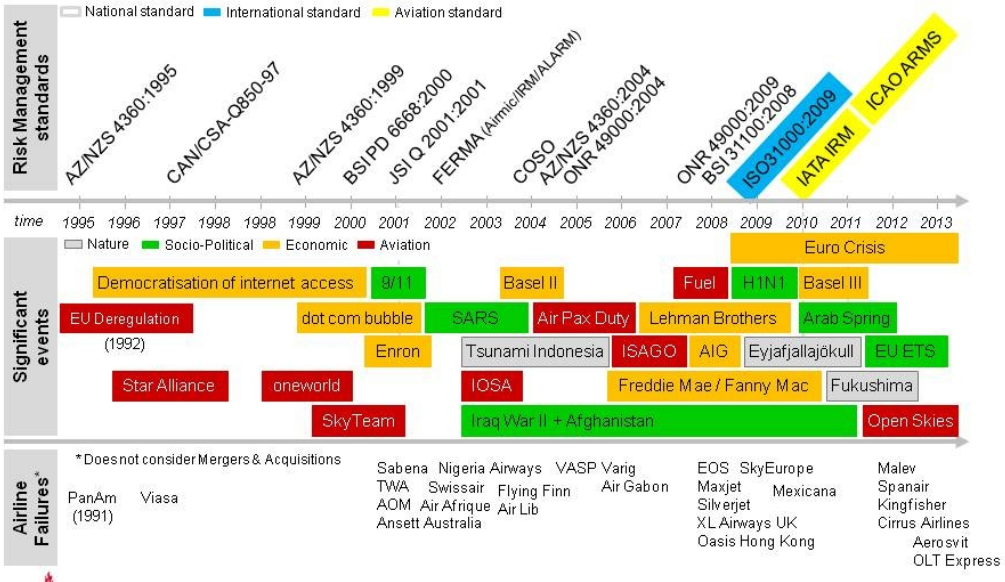


Source: Albers, et al., 2005

CITY UNIVERSITY LONDON | Phd Holistic Risk Management in Commercial Air Transport
Airline Risk Management Framework
by Paulo Nunes – 22nd August 2013

5

Yet over time, risks and risk management standards have increased in volume and sophistication



CITY UNIVERSITY LONDON | Phd Holistic Risk Management in Commercial Air Transport
Airline Risk Management Framework
by Paulo Nunes – 22nd August 2013

6

Research shows that only few airlines consistently apply recognized risk management standards

General Conclusions (from literature)

- Between 1995 and 2013 at least 8 national or international industry-neutral risk management standards were published and subsequently revised and updated
- The most recent, and internationally recognized standard is ISO 31000:2009, initially based on the Australian and New Zealand versions of their national documents
- Two aviation-specific standards were published in 2010, one by IATA and one by ICAO
- IATA's Integrated Risk Management approach has – by IATA's own words – been difficult to implement at airlines, whose acceptance has been low
- The ICAO standard is mostly focussed on safety and operations as it was "set up in order to develop a new and better methodology for Operational Risk Assessment"

Specific conclusions (from research conducted)

- Of the 100 largest airline groups (by revenue), 8 do not refer to risks or risk management in their 2011 Annual Report; another 22 do not publish any regular report
- 32 airlines do not mention any specific standard used for their risk management activities; the remaining 38 cite one or more risk management standard
- 28 airlines have statements citing COSO for their risk management and internal control activities (including all US-based stock listed airlines as part of their SEC reporting guidelines and requirements)
- 4 refer to the use of ISO31000: Singapore Airlines, Thai Airways, South African Airways and Cargolux
- 2 airlines quote AS/NZS 4360:2004: Cathay Pacific and Air New Zealand
- Qantas mentions the use of ISO31000:2009 and AS/NZS 4360:2004; Finnair cites COSO and ISO31000
- Ryanair and Aer Lingus cite the Turnbull Guidance

A number of reasons can justify the limited use of risk management techniques in the airline business

Potential reasons for limited use of risk management :

- Lack of leadership and commitment
- Lack of knowledge and understanding of concepts
- Lack of interest and/or other priorities
- Lack of resources (financial, human, technical, time)
- Lack of proper and/or industry-specific guidance material, and/or acceptance of existing material
- Lack of training on tools and techniques
- Lack of cooperation between industry bodies
- Internal and/or external opposition
- Seen as another bureaucratic hurdle
- Time intensive exercise
- Voluntary nature of risk management (no enforcement or certification requirement)
- Decisions taken and/or imposed by other entities (shareholders, stakeholders)

and...

Limited visibility of results
(if results were largely visible, topic would get attention, resources and commitment from upper management)

This project recommends an airline specific approach to ISO31000, the most recent and used standard

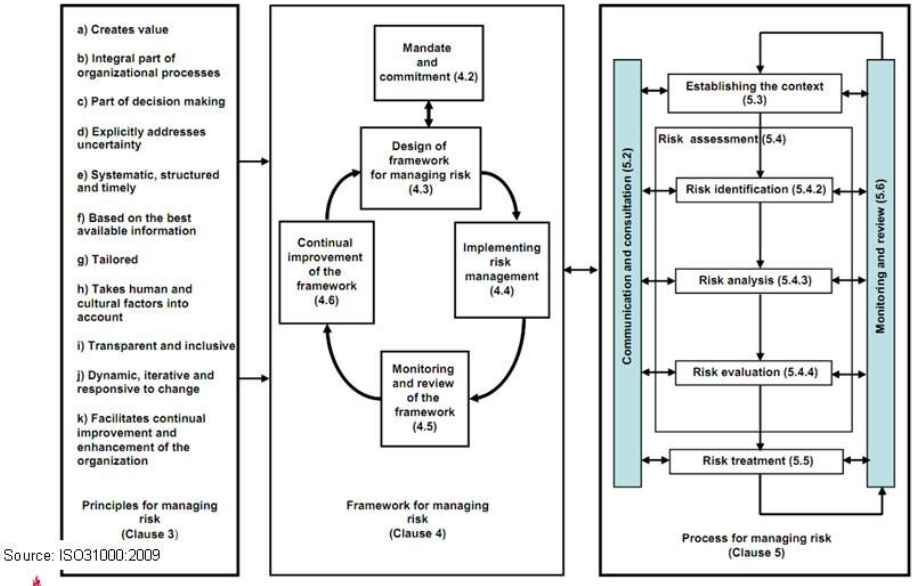
Why ISO31000 as chosen standard:

- It is the most recent standard
- It is an internationally valid and recognized standard
- It is industry neutral and has been implemented in many industries, geographies and company sizes
- Enables a holistic view of risk inside the organisation, but also overwhelming to others
- It can be flexibly adjusted to the airline environment
- Some airlines have already successfully applied this standard
- IATA's Integrated Risk Management Standard gathers input from ISO31000, but has found difficulties in getting accepted and implemented

Why an adapted framework and not a new standard:

- More than a new risk management standard or model, this project proposes an industry-specific framework where an existing risk management standard can be applied
- Guide 73 of ISO31000 defines a risk management framework as: "**set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management** throughout the organization"
- Airlines do not need something new (again), but rather something that works – which is easily understandable, implementable and effective, without consuming a vast amount of resources
- Making such a framework airline-specific is the best way to address their industry-specific problems

ISO31000 outlines a set of principles, that guide the framework the risk management process interacts with



Source: ISO31000:2009

Contents

1. Introduction: overview of definitions, standards and airline practices
2. **Goals for a proposed framework adaptation**
3. Proposal for a newly adapted airline risk management framework
4. Annex: Step-by-step details

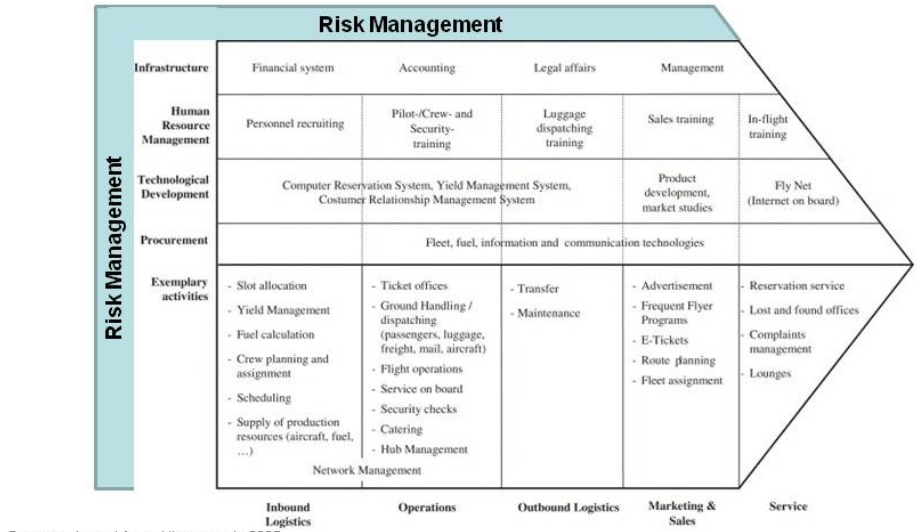
The ultimate goal of this proposal is to help airlines better manage risk and therefore their daily business

Goals:

- Have a risk management framework that is:
  - **Easily understandable**
  - Based on **international best practice**
  - **Industry-specific**, yet still customizable by each airline
  - **Adjustable** to the needs and requirements of each airline
- Help airlines introduce risk management practices, to:
  - **Identify, assess and manage all risks** (or as many as possible), without focussing on one area in particular
  - Focus on **internal and external risks** to their environment, but also **involve their stakeholders** in the risk management process
  - Help airlines **achieve goals** and create better management practices
  - **Improve resilience** to face a tough, changing and challenging business and operating environment

Reduce risk
in daily operation
and management

This way risk management should become an ever present activity in the airlines' value chain



Source: adapted from Albers, et al., 2005

Ideally this holistic approach should enable airlines to involve all stakeholders in the process

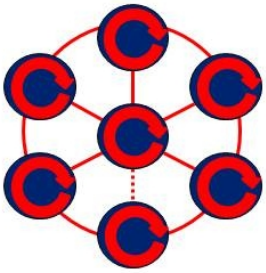
From...

Legend:
— Traditional business relationships
···· Business relationship with legal constraints

Status quo:

- Limited or no risk management within the airline
- No risk-based relationships with stakeholders

To:



Legend:
Risk-aware business relationships
Implemented risk management practices

Vision:

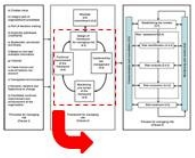
Achieve better risk management...

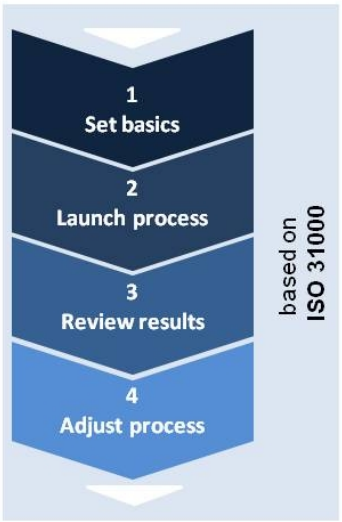
- **within the airline**
- **within all stakeholders**
- **in the industry** *...utopia?*

Contents

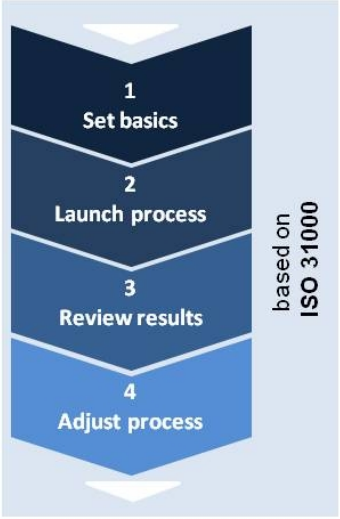
1. Introduction: overview of definitions, standards and airline practices
2. Goals for a proposed framework adaptation
3. **Proposal for a newly adapted airline risk management framework**
4. Annex: Step-by-step details

The adaptation of the ISO31000 framework to the airline environment must keep simplicity as cornerstone





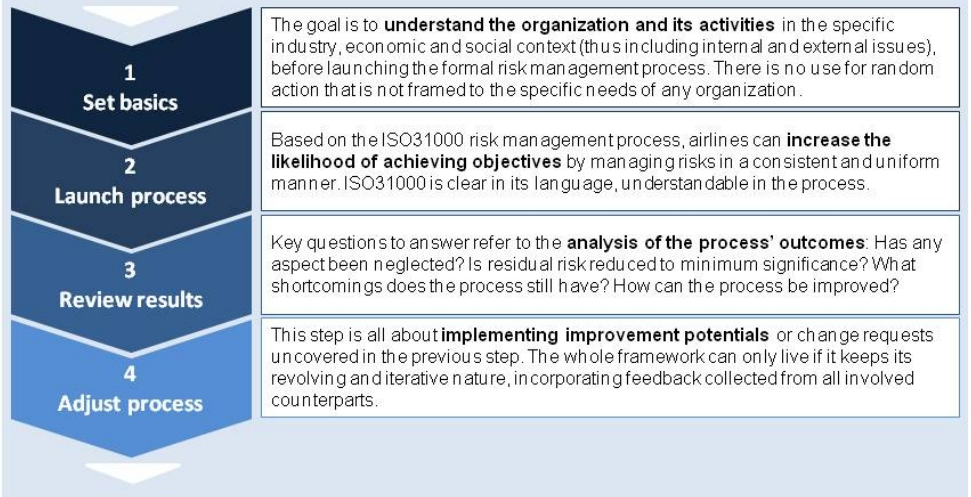
The adaptation of the ISO31000 framework to the airline environment must keep simplicity as cornerstone



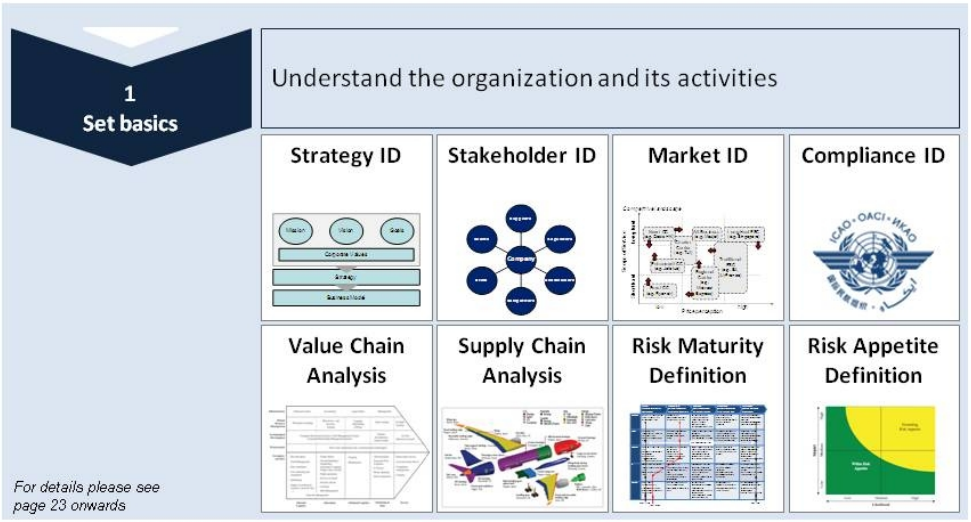
Key elements:

- **Simplicity**
  One key criticism to other models is that they are too complex and heavy; "simplicity by design" should be at the forefront for easier understanding and acceptance.
- **All-embracing**
  The airline business is already highly regulated and some areas are very good in managing their own risks, yet there is rarely a common and uniform approach to all risks the airline is exposed to. This new framework should be able to accommodate all sorts of risks, regardless of their nature.
- **Revolving**
  This is a dynamic industry impacted by all types of issues, from geo-political events to technological developments. Reviewing and adjusting the risk management results, processes, responsibilities is key.
- **Based on ISO31000**
  It is the latest, internationally recognized, industry-neutral and most intuitive standard. It contains a clear process description and harmonized language making it a good base for an airline specific framework.

By being all-embracing, it will be possible to address issues from all operating and non-operating areas



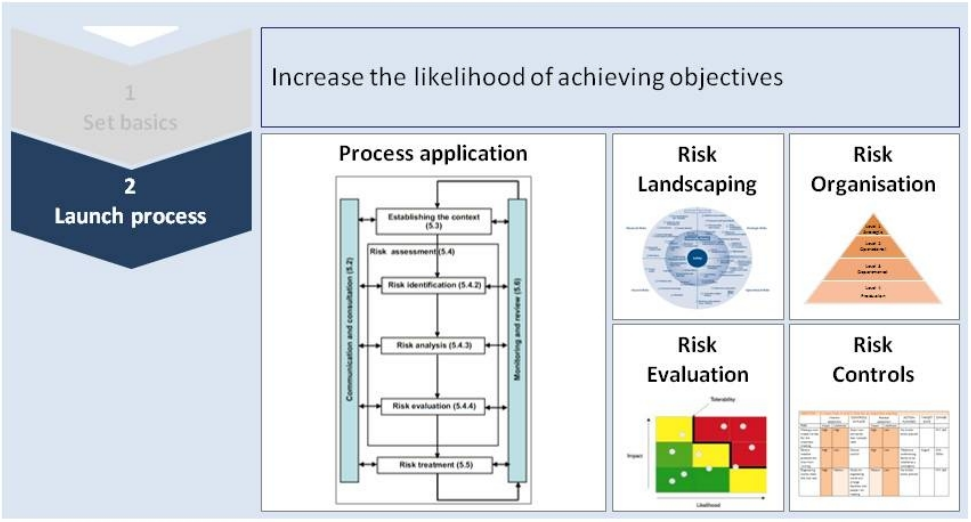
It is essential to start by capturing a detailed picture of the airlines' internal and external environment



CITY UNIVERSITY LONDON | Phd Holistic Risk Management in Commercial Air Transport
Airline Risk Management Framework
by Paulo Nunes – 22nd August 2013

19

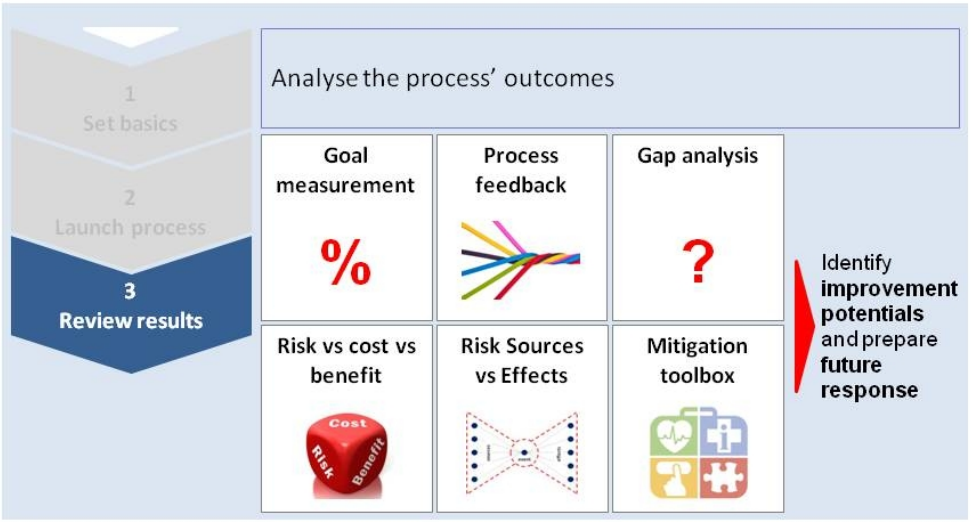
Using ISO31000 will help identifying, categorizing and prioritizing risks



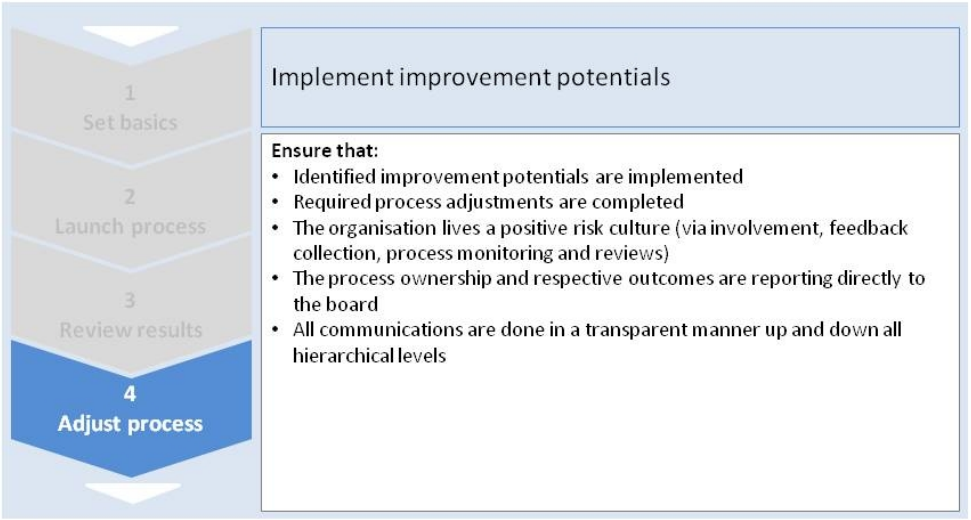
CITY UNIVERSITY LONDON | Phd Holistic Risk Management in Commercial Air Transport
Airline Risk Management Framework
by Paulo Nunes – 22nd August 2013

20

As revolving and iterative process, improvement potentials must be gathered from all sources



The success of this process can only be guaranteed if identified improvements are implemented and lived

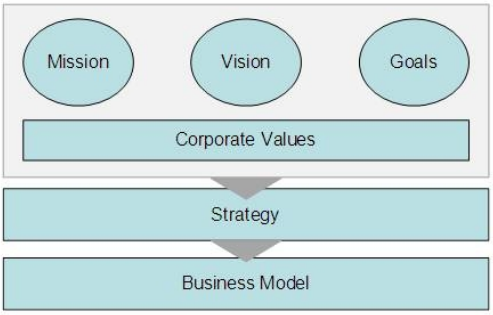


Contents

1. Introduction: overview of definitions, standards and airline practices
2. Goals for a proposed framework adaptation
3. Proposal for a newly adapted airline risk management framework
4. **Annex: Step-by-step details**

Details

Set Basics
Strategy ID

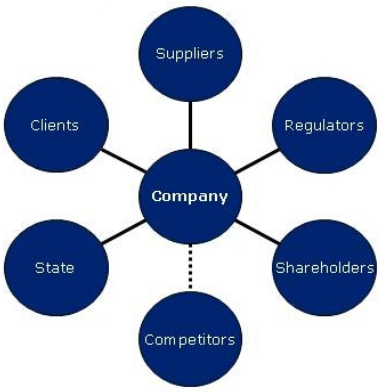


Key elements

- Collect the airlines' mission statement, overall vision, goals and corporate values. This shows **what the airline is or wants to be, when and how**. Normally contained in the Strategic Plan and/or Business Plan. Should show pre-defined quantified targets.
- A strategic direction should be documented, showing **how the airline wants to achieve its goals**. If not available, outline one based on interviews with key stakeholders, internal management workshops, etc. Without a corporate strategy it will be difficult to design a risk management strategy, risk tolerance and attitude.
- **How are all available resources being combined** – or how should they be combined to fulfil the strategy the airline has outlined? Is this working properly or should amendments be made?
- This step **should include a thorough SWOT and PESTEL analysis** – to complement and prepare the elements of the following steps

Details

Set Basics
Stakeholder ID



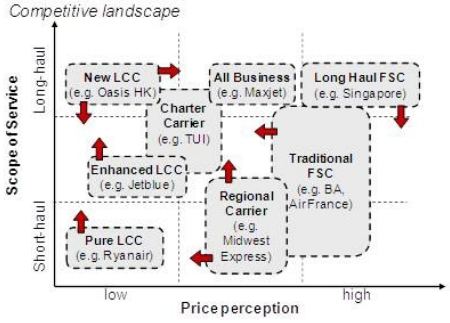
Key elements

- **Stakeholders have needs and requirements**, take decisions and act in the market place in a manner that can impact a companies' life.
- **Identifying who they are, what they want,** how they can impact an airlines operation, and establishing a close communication line with them is already half-way to help addressing potential risks.
- From an airlines' perspective, not only are regional and national authorities, companies and society relevant of where the airline is based, but also where it flies to – virtually globally!
- Associated to this is the management of these stakeholders: from our own organisation, who communicates with each stakeholder? Is there a direct communication line?

Details

Set Basics
Market ID

Competitive landscape



Key elements

- This is about competitors, customers and our own position in this landscape. How do we position ourselves in the market to attract (and serve) our customers?
  - Who are our **competitors**?
  - What is our/their relative **market share** in each market we serve?
  - What **development plans** do they have?
  - Who are current and potential **partners**?
  - How large is the **customer base** by market?
  - Do we serve all **segments** or focus on few?
  - What merger & acquisition **movements** are going on – are we predators or prey?

Details

Set Basics
Compliance ID

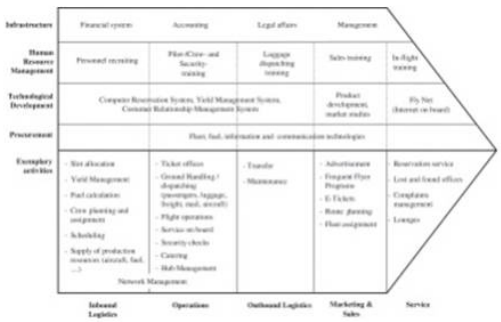
Key elements

- A number of regional, national, international authorities oversee air transport operations, establishing legal, operational and financial rules for the business
  - Are we aware of and compliant with all these **rules and regulations**?
  - What are the **implications of non-compliance**?
  - Do we have a formal unit to manage all compliance-related issues?
  - Who represents us at these bodies?
  - Can we influence the decisions and rules taken by these bodies?

CITY UNIVERSITY LONDON | Phd Holistic Risk Management in Commercial Air Transport
Airline Risk Management Framework
by Paulo Nunes – 22nd August 2013 27

Details

Set Basics
Value Chain Analysis



Source: Albers, et al., 2005

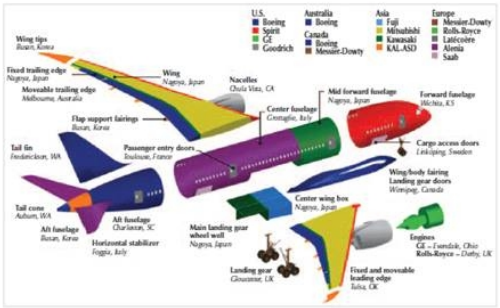
Key elements

- Each airline has its own *modus operandi* and thus a different – more or less complex – **value chain**.
- Mapping out all elements in this chain, describing current **processes** and the ideal situation will help identifying and managing potential gaps and shortcomings.
- This should include **outsourced operations**, the **legal and contractual aspects** related to those outsourced activities.
- Having clearly assigned **roles and responsibilities** for each of the tasks enables quicker decision making and communications.
- Note: a generic airline value chain does not contain risk management as one of its elements.

CITY UNIVERSITY LONDON | Phd Holistic Risk Management in Commercial Air Transport
Airline Risk Management Framework
by Paulo Nunes – 22nd August 2013 28

Details

Set Basics
Supply Chain Analysis



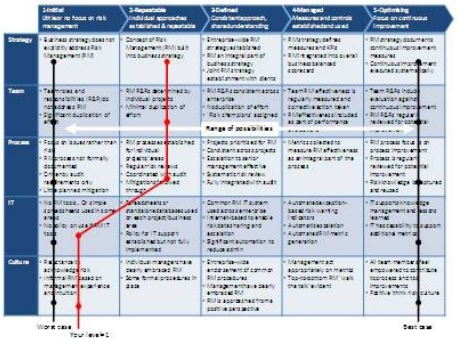
Source: boeing.com

Key elements

- Like building an aircraft, where parts are sourced all over the world, airlines have a vast range and diversity of suppliers. The failure of one may impact the whole operation of the airline.
- The suggestion is to build up a catalogue of current and potential suppliers, containing information on what their part in the airlines' business is, how they manage risks, and how they can affect the airlines' operation.
- For the most critical ones, establish partnership agreements either between similar client organisations or alternative suppliers to meet potential disruptions.
- Taking risk management a bit further would imply suppliers managing their risks according to same (or similar) standards, too, in order to have total alignment.

Details

Set Basics
Risk Maturity Definition



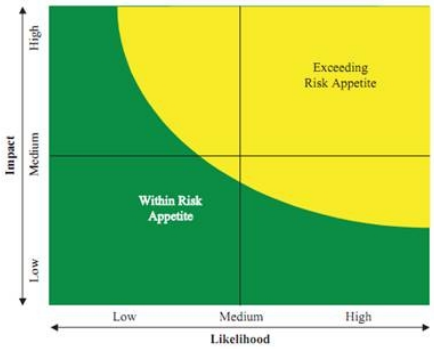
Source: Baxter, 2010, p. 193

Key elements

- If the organisation does not understand the concept of risk or the need for a formal risk management process, than that is half-way for failure.
- There a number of ways to formalise a companies' risk maturity, either using online resources, consultants or questionnaires and assessment templates (as proposed by Baxter).
- Such templates look into various areas across the organisation, from strategy to processes, team to culture.
- Goal is to identify less risk mature areas to focus on them.
- Baxter suggests "you are only as good as your weaknesses".

Details

Set Basics
Risk Appetite Definition

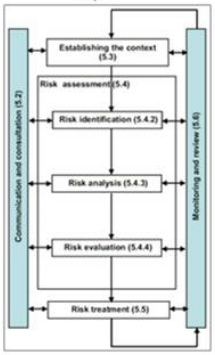


Key elements

- Defining risk appetite is about **setting the boundary of what is and what is not acceptable** for the organisation .
- By creating such a threshold it will be easier to **eliminate risks** that fall beyond that level, focussing and prioritising risks that fall within the acceptability range.
- As for the maturity model, there are a number of pre-formulated templates and online resources that can be used for establishing this risk appetite level.
- As it is a corporate statement, related to the company itself and not therefore not the industry it is working in, it can not be made industry-specific.

Details

Launch Process
Standard application



Source: ISO31000:2009

Key elements

- This is where the original ISO31000 process starts to be applied, using its seven steps:
  - **Establish the context** (based on previous steps)
  - **Identify risks**
  - **Analyse risks**
  - **Evaluate risks**
  - **Treat risks**
  - (parallel and constant) **Communicate & consult**
  - (parallel and constant) **Monitor & review**
- Interviews, workshops, brainstorming sessions, formal reporting guidelines, database monitoring, etc, all contribute to this step.
- Forms and formats for reporting purposes should be defined, involving all participating units to get their buy-in and acceptance.
- Identify **Key Risk Indicators** and means to measure them; set targets and objectives.

Details

Launch Process
Risk Landscaping

Source: Zea, M., 2002. Is airline risk manageable?. *Airline Business*, April

Key elements

- A typical airline risk landscape includes internally and externally driven items that can be of 4 different natures (strategic, operational, financial or hazard-related risks).
- Each airline may build its own landscape structure with as many categories as needed, to depict the number of risk factors it has identified in the previous process.
- While this does not show any severity or impact levels, it enables the visualisation of the entire risk landscape, showing the most voluminous areas.
- Safety is normally at the centre of each operation – as depicted – but an airline is not safe by decree; all actions need to be taken to ensure consistent safety records.

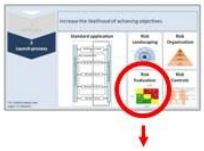
Details

Launch Process
Risk Organisation

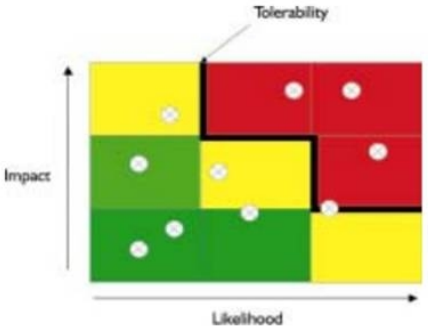
Key elements

- Some airlines tend to decentralise risk management, others tend to have a centralised unit coordinating the entire process and directly reporting to the board.
- In any case, given that there are various levels of risks and there should be the possibility of escalating risks down and upwards in the organisation, it is proposed to organise risk response around source and impact level:
  - Strategic risks should be handled by upper management
  - Operational risks are responsibility of senior management
  - Departmental risks are to be managed by middle-management, and
  - Production-related risks should be managed by individual operational units

Details



Launch Process
Risk Evaluation



Key elements

- Depending on the sophistication and management style of the organisation, a quantitative and/or qualitative risk evaluation needs to take place along aspects of likelihood and impact.
- It is suggested to add a third dimension on speed of occurrence, showing that even less likely events but with high impact and high speed of development should be looked at.
- The tolerability level depicted here is related to the risk appetite limit defined earlier.
- Result is to re-depict the risk landscape to show what are critical elements and focus resources on the resolution of those.
- Risk visualisation and prioritisation are the ultimate goals of this step.

Details

Launch Process
Risk Controls

OBJECTIVE – To travel from A to B in time for an important meeting

	Inherent assessment		CONTROLS IN PLACE	Residual assessment		ACTION PLANNED	TARGET DATE	OWNER
RISK	Impact	Likelihood		Impact	Likelihood			
Missing a train makes me late for the important meeting	High	High	Catch train one earlier than I actually need	High	Low	No further action planned		M.Y. Self
Severe weather prevents the train from running	High	Low	Cannot control	High	Low	Telephone conferencing facility to be installed as a contingency	August	A.N. Other
Engineering works make the train late	High	Medium	Check for engineering works and arrange flexibility with people I am meeting	Medium	Low	No further action planned		M.Y. Self

Key elements

- Reporting is key in this process. The more detailed such reports are the easier it will be to track responsibilities on actions taken (or not taken).
- Ideally such reports are tool-based for easier and automatic handling, avoiding manual typing in preformatted templates and spreadsheets.
- Predefined risk controls help creating a uniform treatment description and allocate tasks and responsibilities.
- Adding "residual risk assessment" enables the depiction of the risk landscape before and after risk mitigation measures have been implemented. Ideally a left-wards movement on the likelihood-impact graph should become visible.

Source: HM Treasury, 2004. *The Orange Book - Management of Risk - Principles and Concepts.* London: HM Treasury.

Details

Review Results
Goal Measurement

%

Key elements

- Measure Key Risk Indicators (identified before) and compare them against predefined targets and objectives.
- Launch benchmarking exercise (if possible) among partner airlines, alliances, or industry (if data is harmonized and available).
- Gather corporate Key Performance Indicators and overall company goals.
- Compare Key Risk Indicators with corporate Key Performance Indicators to understand if the introduction of risk management contributed to the achievement of company goals.

Details

Review Results
Process Feedback

Key elements

- Check process effectiveness by collecting feedback from all internal and external contributors
- Feedback can be from one-to-one conversations, anonymous feedback forms, group workshops, company wide surveys, etc.
- Review if identified risk landscape is complete and/or accurate and list what is missing
- Identify process improvement potentials, resource availability, commitment and allocation, review responsibility assignment

Details

Review Results
Gap Analysis

Key elements

- The previous two elements ('Goal Measurement' and 'Process Feedback') enabled understanding the achievement of planned results, comparing these to pre-defined goals, as well as looking at other organisations, while gathering feedback on the process. All this contributes to the identification of possible gaps in the process and its outcomes.
- Therefore, it is relevant to know:
  - What is missing?
  - Why is this happening?
  - Can the process be adjusted?
  - What has to be changed?
  - What is needed to change it?
  - How long will it take?
  - Will the change be effective?

Details

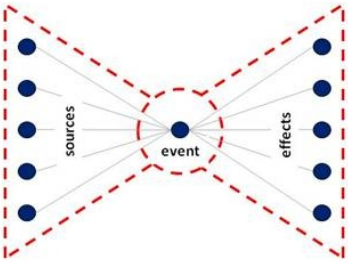
Review Results
Risk vs Cost vs Benefit

Key elements

- A cost benefit analysis to the key risks, their mitigation measures and expected benefits should be conducted to understand if it is economically sensible.
- This exercise should not be conducted solely by the risk owners, as their perceptions might be skewed (every risk must be mitigated, regardless of their impact).
- Instead, it should be coordinated by the risk management unit, getting help from cost-benefit experts in the organisation (e.g. economic studies) and/or other third-parties to get their external views on the issue.
- While the result of this should not be a go/no go decision, it should rather highlight the involved costs, expected benefits (or avoided losses) to the risks that have been identified and addressed.

Details

Review Results
Risk sources vs effects



Key elements

- For identified risks (at least for those considered top priority) understand what are the triggers contributing to its occurrence and check the effects that this might have within or around the company
- Review interdependencies and correlations between different risk events, sources and effects: each source is triggered by a number of other events; each effect triggers further issues.
- To help visualize the complexity of the risk landscape, a graphical depiction of all risks, sources and effects could be produced.
- This process helps streamlining the whole risk landscape and reduce it to the core and essential elements, eliminating duplications and redundancies.

Details

Review Results
Mitigation toolbox

Key elements

- Collect all possible risk mitigation measures introduced during the whole process, complementing this with other potential measures that have not yet been used, but are available and dominated by internal staff.
- This will build a catalogue of possible mitigation measures that are available upon request.
- If possible, include feedback on the mitigation measures, outlining effectiveness, ease of implementation, speed of mitigation, etc.
- Disseminate among responsible staff, risk champions and include in training exercises.

Estimated time requirement: 6 months – 9 months, depending on airline's size and complexity

1 Set basics		2 Launch process		3 Review results		4 Adjust process	
Strategy ID	1-4 weeks*	Standard application	8 weeks revolving	Goal measurement	2 weeks	Continuous actions	revolving
Stakeholder ID	1-2 weeks*	Risk landscaping	2-3 days	Process feedback	2-3 weeks		
Market ID	1 week* continuous	Risk evaluation	revolving	Gap analysis	1 week		
Compliance ID	2 weeks* continuous	Risk controls	4 weeks	Risk vs cost vs benefit	2 weeks		
Value Chain Analysis	2-4 weeks*	Risk organisation	1 week	Risk sources vs effects	2 weeks		
Supply Chain Analysis	2 weeks* continuous			Mitigation toolbox	1-2 weeks		
Risk Maturity Definition	1 week						
Risk Appetite Definition	1-4 weeks						

** Duration depends on pre-existing material; can be performed in parallel to other tasks*

Contacts

Paulo Nunes

E-mail: paulo.nunes@nyb.pt
Phone: +351.96.2551186

Thank you for your feedback!