



Universitetet
i Stavanger

**DET SAMFUNNSVITENSKAPELIGE FAKULTET,
HANDELHØGSKOLEN VED UIS
MASTEROPPGAVE**

STUDIEPROGRAM:
Siviløkonomstudiet
Spesialisering i Risikostyring

Opgaven er skrevet innen emnet risikostyring, og er ikke konfidensiell

TITTEL:

ENGELSK TITTEL:

**Improving the Communication and Control of
Operational Risk Profiles**

Forfatter: Anders Eliesen

Veileder:

Studentnummer:

213428
.....

Navn:

Anders Eliesen
.....

OPPGAVEN ER MOTTATT I TO – 2 – INNBUNDNE EKSEMPLARER

Stavanger,/..... 2012

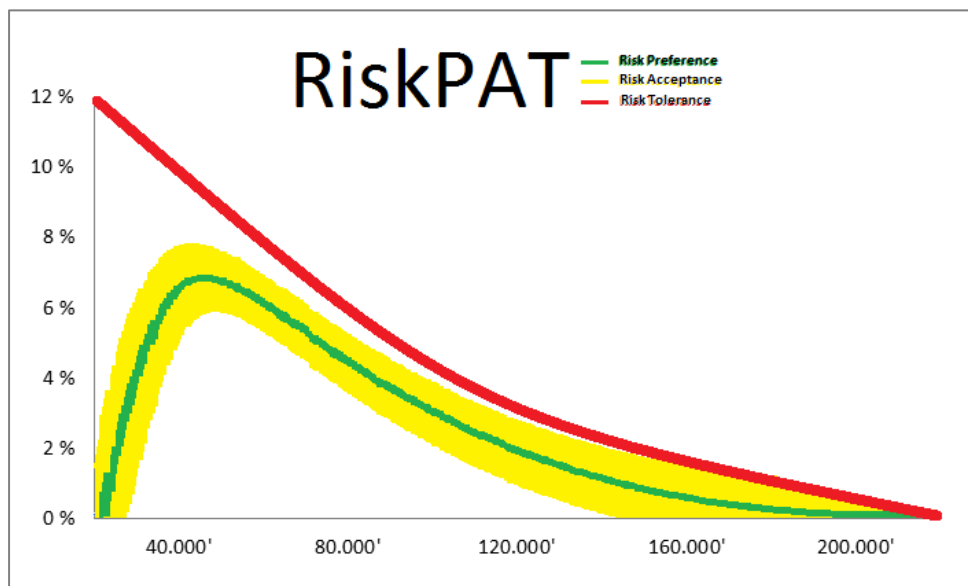
Underskrift administrasjon:.....

Improving the Communication and Control of Operational Risk Profiles

By: Anders Eliesen

Student no.: 213428

June 15, 2012



Universitetet
i Stavanger

Task Description

This thesis aim to explore the field risk profiles within organizations. It will focus on how risk profiles are currently communicated and controlled through terms like “risk appetite” and “risk tolerance”. Ultimately, the thesis aims to give a contribution to the area by either finding new ways or improve the ways that risk profiles are expressed status quo.

Guidance Counselor: Frode Bø

Executive Summary

This thesis takes a hard look on the present techniques and methods that are used for communicating and controlling risk profile to find improvements. The popular term “risk appetite” is dismissed and replaced with a new concept; RiskPAT.

RiskPAT is a tool that is based on the principle to help an organization gain benefits by making it state three values; risk preference, risk acceptance and risk tolerance. By stating a risk of preference and its allowed volatility (respectively, risk preference and risk acceptance) and the limit of risk that the external environment tolerates (risk tolerance), I argue that an organization can gain substantial benefits both internally and externally.

The implementation process of RiskPAT benefits the internal environment of the organization greatly by optimizing it for operational risk management. Measuring techniques are thoroughly improved to optimize communication of risks and preventing problems with ambiguity. These improvements consist of dismissing risk maps in favor of individual risk distributions derived from Bayesian networks and dismissing all other metrics than amounts when measuring. By continuously measuring the individual risks and ensuring their compliance with the RiskPAT, the board gets a clearer image of the true operational risk profile which further increases their control.

The reaped benefits of having implemented RiskPAT are equally bountiful from the external environment. Increased control over operational risks are highly sought after, and displaying this to investors and rating bureaus will definitely cause benefits through increased capital and better ratings. The terms of RiskPAT can effortlessly be controlled, and any false statements will easily be revealed. This is what makes it such a good tool externally too. The RiskPAT will help the external environment to find organizations that have good operational risk management by comparing their risk preference with the risk tolerance. If a financial organization has a risk preference above their risk tolerance, they are undoubtedly more vulnerable to volatility than an organization with its risk preference below the risk tolerance. This scenario ultimately is in favor of the latter organization which most likely would attract more investors.

The RiskPAT could be the future of communicating and controlling risk profiles, and the authorities would be wise to find ways to incentivize this throughout the industry.

Acknowledgements

The work on this Master Thesis has been carried out at The Faculty of Social Sciences at the University of Stavanger.

This Thesis would not have been possible without the help and support of several people. I wish particularly to express my gratitude to Frode Bø, who has been my guidance counselor. He has been incredibly helpful and offered invaluable assistance, and guidance, with his extensive understanding of operational risk management. By continuously challenging me and dedicating extensive amounts of his personal time, he has made me raise this Thesis to a level that would not have been achievable otherwise. I would also like to extend my gratitude to Lasse Berg Andersen and David Häger at the University of Stavanger for the inspirational lectures they have held and their guidance within the field of risk management throughout my studies at the university. An extended gratitude is also extended to Bjørn Tore Larsen, CORO at DNB, for informative reflections, which has been very valuable for the Thesis. Finally, I wish to thank my family and friends for the support and help that they have granted and all of the respondents to my survey.

Thank you. This thesis could not have existed without your help and support.

Anders Eliesen

June 15, 2012

Stavanger, Norway

Table of Contents

- Task Description IV
- Executive Summary V
- Acknowledgements VI
- Table of Contents VII
- List of Abbreviations..... IX
- List of Figures..... X
- Introduction and Motivation..... 1
- Part I - Current Practice of Expressing Risk Profiles - 3
 - 1.1 Introduction..... 4
 - 1.2 Definitions of Risk Appetite..... 6
 - 1.2.1 Publicly available definitions 6
 - 1.2.2 Former discussion on defining risk appetite 8
 - 1.3 Current Practice for Measuring and Communicating Operational Risks 10
 - 1.3.1 Regulatory requirements 10
 - 1.3.2 Measuring and expressing operational risk 11
 - 1.4 Survey on the use of Risk Appetite in Norwegian Banks..... 13
 - 1.4.1 What I wanted to find out 13
 - 1.4.2 Survey analysis and findings..... 14
 - 1.5 Conclusion 26
- Part II - Improving the Risk Terminology - 27
 - 2.1 Introduction..... 28
 - 2.2 Dismissing “Risk Appetite” from the Risk-Terminology 29
 - 2.3 Searching for Alternative Terms..... 31
 - 2.3.1 Learning from the mistakes of risk appetite 31
 - 2.3.2 Controlling risk profiles in the petroleum industry 32
 - 2.3.3 Revealing the new terms..... 35
 - 2.4 RiskPAT: A New Concept for Managing Risk Profiles 36
 - 2.4.1 Brief preview of RiskPAT 36
 - 2.4.2 The contribution of each term 37
 - 2.4.3 Applying the new concept..... 38
 - 2.4.4 Additional notes and opportunities 41
 - 2.4.5 Pitfalls, and ways to avoid them..... 46
 - 2.4.6 Summarizing RiskPAT 47

| | |
|---|-----|
| 2.5 Conclusion | 48 |
| Part III - Optimizing the Benefits of RiskPAT - | 49 |
| 3.1 Introduction..... | 50 |
| 3.2 Incentives for Implementing RiskPAT..... | 51 |
| 3.2.1 The financial crisis | 51 |
| 3.2.2 The Basel II framework: Basic indicator approach and Standardized approach..... | 54 |
| 3.2.3 The Basel II framework: Advanced measurement approach | 55 |
| 3.2.4 Current incentives for mitigating risk through the new concept..... | 57 |
| 3.3 Internal Communication and Control of the Risk Profile | 58 |
| 3.3.1 Selecting the best metric for communication | 58 |
| 3.3.2 Risk maps in the financial industry..... | 60 |
| 3.3.3 Risk distributions | 62 |
| 3.3.5 Bayesian networks..... | 64 |
| 3.4 Conclusion | 69 |
| Part IV - Reviewing RiskPAT and the way forward - | 71 |
| 4.1 Reviewing the Thesis | 72 |
| 4.2 Bank E's Implementation of RiskPAT..... | 73 |
| 4.2.1 Setting the risk preference and the risk acceptance..... | 73 |
| 4.2.2 Finding Bank E's risk tolerance..... | 73 |
| 4.2.3 Internal environment and risk identification | 74 |
| 4.2.4 Breaking down the general risk preference | 75 |
| 4.2.5 Reporting and measuring compliance..... | 76 |
| 4.2.6 Publicly stating the RiskPAT and post-implementation benefits | 77 |
| 4.3 Concluding Remarks and the Way Forward..... | 79 |
| - Appendix - | 81 |
| Appendix 1: Definitions from M. Leitch's Article | 82 |
| Appendix 2: Survey Information | 83 |
| The questionnaire | 83 |
| The data..... | 83 |
| Appendix 3: Survey Report..... | 85 |
| Appendix 4: Survey Routing Map..... | 104 |
| Appendix 5: Adjusted Graphs..... | 105 |
| References..... | 106 |

List of Abbreviations

| Abbreviation | Explanation |
|---------------------|--|
| ERM | Enterprise Risk Management |
| COSO | Committee of Sponsoring Organizations of the Treadway Commission's |
| IRM | The Institute of Risk Management |
| ISO | The International Organization for Standardization |
| BS | British Standards |
| KRI | Key Risk Indicators |
| BIA | The Basic Indicator Approach |
| SA | The Standardized Approach |
| AMA | The Advanced Measurement Approach |
| BEICF | Business Environmental and Internal Control Factors |
| ALARP | As Low As Reasonably Practicable |
| PIT | Point-in-time |
| TTC | Through-the-cycle |
| CDO | Collateralized Debt Obligation |
| CDS | Credit Default Swap |
| VaR | Value at Risk |
| RiskPAT | Risk-Preference/-Acceptance/-Tolerance |

List of Figures

| Page no. | Figure no. | Caption |
|----------|------------|--|
| 1 | I | Risk appetite in Ernst & Young's survey |
| 12 | 1.1 | Risk Map |
| 15 | 1.2 | How do you know the terms «risk tolerance and «risk appetite»? |
| 16 | 1.3 | Different perceptions of risk tolerance and risk appetite |
| 17 | 1.4 | Risk appetite as a maximum limit |
| 17 | 1.5 | Risk appetite as a specific level |
| 18 | 1.6 | Risk tolerance as a maximum limit |
| 19 | 1.7 | Risk tolerance as an optimal level |
| 20 | 1.8 | To what degree is "risk appetite" and/or "risk tolerance" used on a daily basis in the organization? |
| 21 | 1.9 | How risk appetite and tolerance are used in strategies |
| 22 | 1.10 | How organizations' risk profile is expressed |
| 23 | 1.11 | Operational risk-strategies in Norwegian banks |
| 24 | 1.12 | How many operational risks have Norwegian banks identified? |
| 24 | 1.13 | Are the identified risks quantified? |
| 31 | 2.1 | Different plausible conceptions of the term "risk appetite" |
| 33 | 2.2 | Risk Acceptance Criteria |
| 34 | 2.3 | ALARP |
| 37 | 2.4 | The concept of RiskPAT |
| 40 | 2.5 | Low risk preference/high risk tolerance |
| 41 | 2.6 | High risk preference/Low risk tolerance |
| 45 | 2.7 | An edited illustration of the PIT- and TTC-method (Sparebank 1 SR-Bank. 2012). |
| 47 | 2.8 | An illustration of RiskPAT |
| 52 | 3.1 | Activity in rating bureaus from 2003-2007 (Lasse B. Andersen. 2011). |
| 52 | 3.2 | CDO ratings' change over previous years (Lasse B. Andersen. 2011). |
| 55 | 3.3 | Common operational loss distribution (Häger, 2011) |
| 59 | 3.4 | A simple conversion table |
| 61 | 3.5 | Placement of operational risks in a risk map |
| 62 | 3.6 | Risk map representing risk from Chapter 3.3.2 |
| 63 | 3.7 | Risk map with a distribution of the risk from Chapter 3.3.2 |
| 64 | 3.8 | Bayesian network (Häger, 2011) |
| 65 | 3.9 | Bayesian network of a typing error |
| 66 | 3.10 | Sensitivity analysis |
| 67 | 3.11 | Bayesian network of a typing error in bar format |
| 68 | 3.12 | Seasonal aspect with Bayesian networks |
| 74 | 4.1 | RiskPAT in Bank E |
| 75 | 4.2 | Bayesian network and loss distribution of the risk of wrongly giving advice. |
| 76 | 4.3 | The actual state of the operational risk (black line) compared with the risk preference (green line) and its surrounding risk acceptance (yellow zone) |
| 77 | 4.4 | The risk's Bayesian network and loss distribution after the risk mitigation |

Introduction and Motivation

In the aftermath of the recent financial crisis, financial institutions have been criticized for being too reckless with their risk profile and for lacking knowledge of how to express it. This has boosted the interest for further research on how to control and communicate the risk profiles, which is currently being done with the organizations stating their “risk appetite”. A recent survey made by Ernst & Young (E&Y. 2011) of 62 international banks shows us that 96 % of the banks have increased their focus on risk appetite after the financial crisis, which further proves this interest.

My motivation to write this thesis derives mainly from E&Y’s survey but also through discussions with Frode Bø. According to the survey, 96% of the banks had increased their focus on risk appetite, but when doing a search on the subject, there seem to be no consensus on how to either approach it or understand it. This states the need for a terminology within the

financial industry which efficiently allows proper communication of their risk profile without misunderstandings. The survey further concludes that boards mostly approve the risk appetite instead of being actively engaged in the development of it, and that only 25% of the banks can draw a significant linkage between business decisions and risk appetite (illustrated in Figure I)(E&Y. 2012).

It is interesting to see that most of this sudden increase in interest has appeared after the industry has witnessed real-world scenarios such as the subprime crisis, the Acta verdict and the Terra scandal. Most of these incidents could probably have been reduced, or even been avoided, if all of the concerned parties had a clearer image of the organizations’ risk profile. I will therefore approach this thesis with the intention of identifying and

solving the current problems with risk appetite in the interest of improving financial organizations’ control and communication of their risk profile. Due to the young nature of operational risk management and personal interest in it, the thesis is written specifically for this field.

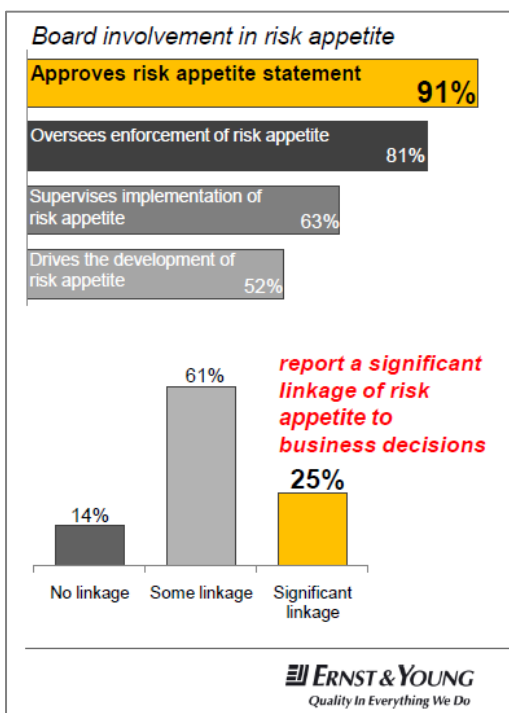


Figure I – Risk appetite in Ernst & Young’s survey (E&Y. 2011)

The first part of this thesis will map the current status of the research within the field. It also includes a survey on how different banks seem to perceive and apply this knowledge to their practices. The second part will discuss and reflect on the first part's findings with regard to the current risk terminology, and conclude on what needs to be done to improve it. In part three, I will discuss how the current practice of risk measurement communicates its results, and how risks ideally should be communicated throughout the company. Finally, I will summarize the thesis through a thorough example and suggest future research within the field in the last part. Information will be gathered through available literature, articles, class lectures and a survey that is sent out to the largest banks in Norway.

Part I
- Current Practice of Expressing Risk Profiles -

1.1 Introduction

Defining, communicating and controlling the risk profile of an enterprise are some of the most essential steps in enterprise risk management (ERM). If a bank develops a method to manage this, it will have taken a huge step towards perfecting their core business, which is to earn money on controlling risks.

The positive effects of properly communicating and controlling the risk profile are not only beneficial for the shareholders, but the organization as a whole. Investors' primary objective is to optimize their income by finding the best possible ratio between returns and risks. If investors could at any time know the true risk profile of an organization, they would be able to take more informed choices which would probably, again, lead to an increased capital in these organizations. The board is interested in finding the same optimized ratio between returns and risks for the organization, but also has an obligation to the society to act ethically according to sound principles such as the Norwegian "Internkontrollforskriften". By having a tool that collects, observes and communicates the risk profile of sub-divisions to the board, the board would have a perfect basis for optimizing risk exposure, practice sound principles for risk management and thoroughly express the correct risk profile to the investors.

Employees and sub-managers could also benefit from a perfected risk profile. Not only would their organization be more secure by being more adaptable to future scenarios, but clearer borderlines between acceptable and unacceptable risks would ease the work for many of the employees. Additionally, funds meant for risk mitigation would be divided more fairly, the workplace would be safer and the solidarity would increase due to the fact that the organization starts operating more as a whole.

The industry knows that successfully controlling and communicating their risk profile can lead to these benefits, which has further led to the development of a tool known as *risk appetite*. It would be wrong of me to lead the reader to believe that risk appetite currently is the perfect tool that leads to the ideal state described in the last paragraph. In fact, risk appetite is currently facing problems that seem to have put this dream-scenario on halt. This thesis seeks to lead any financial organization back on the road towards reaching the ideal state and will therefore start by researching the reasons why risk appetite is not working out.

Several risk managing institutions have defined risk appetite differently, without addressing earlier definitions. Consequently, it is hard to get a clear view on the subject. Chapter 1.2 will

present different definitions of risk appetite which will explain some of the reasons behind the confusion that currently exists.

A proper technique for the communication and measurement of operational risks is paramount when aiming to state the risk profile. If the board has set specific levels and/or goals to reach a certain risk profile, it would be hard to know if these goals are met without these techniques. Chapter 1.3 will briefly explain the current status of some of the most commonly used measurement techniques. The chapter assumes that the reader has a basic knowledge of the Basel II accord.

Ambiguity will often cause ripple effects. Banks and other big companies that are dependent on risk management may have different perceptions of risk appetite, which further has been adapted into their individual operational risk management. I sent out a survey to the 23 largest banks in Norway to learn of their take on the subject of risk appetite. The survey will be presented and analyzed in Chapter 1.4.

Chapter 1.5 will summarize the current status on the use of risk appetite as a tool towards expressing the risk profile. This chapter will, both, briefly summarize the current status and work as a pointer to which problems that will be further reflected on and solved in part two of the thesis.

1.2 Definitions of Risk Appetite

The way that risk profiles are managed now is that the board will generally sort out the enterprise's preferred risk level and express it through a "risk appetite-statement". The statement is then distributed to the company's managers, which in turn breaks it down and translates it into detailed and specific goals for each department. Each department's compliance towards reaching these goals is then followed up by the risk department, which in turn reports any anomalies back to the board. The board then decides if changes or additions should be done to the statement which would start the cycle again. The theoretical idea behind it seems simple and should yield any organization substantial benefits if implemented correctly. However, the simplicity also seems to be a pitfall for the concept due to the fact that a proper definition of the risk appetite has not yet seemed to be established. The lack of a proper definition problem leads to ambiguity already at the beginning of the cycle which causes ripple effects throughout the process. Several institutions have tried to define risk appetite, but there is still no consensus on *one* definition.

Consider this scenario: A nation-wide bank with a developed risk apparatus seeks to implement a "risk appetite-statement" in a hunt to reap all of the benefits that was mentioned in the introduction. The company executes the process exactly in the same way that was mentioned in the last paragraph, but when the statement reaches the sub-managers, who are supposed to break the overall goal into more specific goals for their department, a problem arise; one manager thinks that the "risk appetite-statement" expresses the preferable level of risk, and will therefore adjust the risk exposure to be at exactly this level. Another manager within another department believes that the same statement expresses the maximum limit of risk that is accepted, and will therefore make a huge effort to mitigate the risk exposure anytime the department comes close to the stated level. The board would most likely be unaware of this ambiguity within the organization, which further would lead to an observed risk profile that is inconsistent with the *true* profile. To explain the ambiguity that lead to this problem we would have to take a closer look on the source; how is risk appetite currently defined?

1.2.1 Publicly available definitions

In retrospect one might say that the managers should have consulted a valid risk institution's dictionary for a proper definition, but even these definitions tends to vary. Let us take a look on the definitions that established risk institutions offers on their web page.

Norwegian institutions:

- A search on the homepage of **The Norwegian Ministry of Finance** does not give any definitions, but links to an article concerning the management of the oil fund (Finansdepartementet, 2007). Although there is no clear definition, we could derive their intended meaning through the context. The term “risk appetite” is mostly tied together and treated as a synonym for risk tolerance. It also mentions risk limits in the same sentence, which gives the overall impression that risk appetite is defined as a maximum limit for risk.
- **The Norwegian Central Bank** only lists one reference to the term “risk appetite” from a speech about the state of the economy (Øystein Olsen, 2011). The article use “risk appetite” in a literal sense, which means that the market has had a high exposure to risk during the mentioned period, which is irrelevant for this thesis.
- **The Financial Supervisory Authority of Norway (Finanstilsynet)** cites COSO’s framework for ERM in an article with guidelines to risk management an internal controls (Aamo and Bellamy, 2009). The framework, along with other works by COSO, will be discussed later.

International institutions:

- The aforementioned **Committee of Sponsoring Organizations of the Treadway Commission’s (COSO)** offers several sources to define risk appetite. Firstly, there is their well-known framework for ERM. A detailed definition is given as “...*the amount of risk, on a broad level, an entity is willing to accept in pursuit of value.*” (COSO, 2004). This definition places risk appetite as an amount of risk which the enterprise is willing to accept. The framework mentions later in the same paragraph that risk tolerance is the limit that defines the allowed anomalies of the risk appetite. COSO also recently published a new paper consisting exclusively of thoughts on risk appetite. The paper doesn’t change their former mentioned definition, but expands it as “...*the amount of risk, on a broad level, an organization is willing to accept in pursuit of value. Each organization pursues various objectives to add value and should broadly understand the risk it is willing to undertake in doing so*” (COSO, 2012). In their view, nothing has changed with the term through the last 8 years, and they still see “risk appetite” as a level that the entire enterprise should stride to stay at.

- **The Institute of Risk Management (IRM)** defines risk appetite in their guidance paper as *“The amount of risk that an organization is willing to seek or accept in the pursuit of its long term objectives.”* (Institute of Risk Management, 2011).
- **The International Organization for Standardization (ISO)** does not include a definition in their ISO 31000 from 2009, but defined it in Guide 73, a 2002 publication, as the *“Amount and type of risk that an organization is willing to pursue or retain”* (ISO, 2002).
- **British Standards (BS)** has defined it in BS31100 as *“Amount and type of risk that an organization is prepared to seek, accept or tolerate”* (British Standards, 2008). which is quite similar to ISO’s definition.

The three last definitions have taken a more simple approach to defining risk appetite, and explain it as how much a company is willing to sacrifice in order to fulfill their objectives. More definitions could have been found and quoted, but the point is clear; there is no consensus on how to define risk appetite, either, on its own or relative to any other known expression. This is, however, not the first time that someone tries to define risk appetite. Let us take a look on a former discussion on the problem to see if a definition can be found there.

1.2.2 Former discussion on defining risk appetite

Matthew Leitch, an experienced consultant within uncertainty, has written an extensive article (M. Leitch, 2010) on the matter of defining risk appetite. He quotes several definitions, and specify some misconceptions that the definitions produce. The author seems overall negative towards the whole concept of businesses using risk appetite, which he states through several “misconceptions”. Some of these misconceptions don’t seem properly thought through such as *“That there's one level that is the right one regardless of the decision involved and that this level is determined by some kind of decision making logic. In reality each decision is different and the maximum amount of risk that a decision maker would be willing to take will increase with the predicted rewards.”* (M. Leitch, 2010). Although this statement is true, it is not a valid argument for discarding risk appetite. If the key risk indicators (KRI) which are used in the “risk appetite-statement” of a company included e.g. ratios such as a basic benefit/loss-ratio instead of fixed numbers, the risk appetite would automatically adjust itself to reflect an increased reward. Other misconceptions are, however, more spot on; *“That the maximum level of risk that a decision maker would be willing to take depends on the decision maker's goals. In reality it should depend on what the decision maker expects to receive as a reward,”*

not on what he/she would like to receive.” (M. Leitch, 2010). This misconception is indeed true and works as a valid argument against some of the definitions.

By using the same approach as in the last sub-chapter, Matthew Leitch compares definitions that are published by well-known institutions such as HM Treasury, Lloyds Market and the Oxford Diary (a complete and simplified list of sources and definitions which is quoted directly from the article can be found in Appendix 1), and finds the same results as earlier stated; there is still no clear definition of the term.

Risk appetite is defined by many, and will probably continue to be defined by many more in the hunt for a “better” definition. Whether or not a heavily detailed definition exist is irrelevant as long as businesses cannot agree on a single definition of the term. Without a proper consensus on a definition, it would be impossible to use the term, both, for internal and external communication. The ideology behind risk appetite is great and it definitely fills an empty space in risk terminology. However, it needs to be more strictly defined to leave less room for interpretation if it ever should work as a proper tool for controlling and expressing a risk profile. It may take a long time until an industry-wide definition is established, if ever, which is why it is so surprising that organizations still are interested in using it.

The problems with defining risk appetite as a term do, however, only seem to be one of the barriers to break to improve the control and communication of risk profiles. The current practice of using risk appetite will necessarily include measures to monitor and follow up each departments risk exposure. It is extremely important that both the techniques and the parameters used for measuring risks, minimize the chance of ambiguity, so that anyone can easily understand it. The next chapter will describe the current status of techniques and parameters that are used to measure operational risks.

1.3 Current Practice for Measuring and Communicating Operational Risks

In 1996, Euromoney magazine wrote: *“Banks measure and control credit- and market-risk because they can, not because it is the biggest or the most dangerous risks that they face. Operational risk is bigger and more dangerous, but no one knows what to do with it.”* (Euromoney Magazine, 1996). Both research and awareness have come a long way since then, but not as long as it should be. The problem is much wider than just being able to measure the operational risk in a correct way. It is also important that the results easily can be communicated without misunderstandings. The true challenge lies in finding techniques and parameters that optimizes both of these criteria.

1.3.1 Regulatory requirements

The Basel II framework has led to more regulations on operational risk management. All financial organizations are currently bound to set a regulatory capital aside to hedge for operational losses. In addition, it is also mandatory to implement a set of principles known as “Sound Practices for the Management and Supervision of Operational Risk” (Basel, 2003). This document consists of ten principles which, rather vaguely, describe how organizations should approach operational risk management. Briefly summarized, it states that boards and managers should actively be involved in developing and distributing banks’ risk frameworks. Operational risks should proactively be identified, assessed and controlled/mitigated, and the organization should actively share the operational risk profile so that any market participants can assess it. These principles do not contribute with anything in terms of practically improving the control and communication of a risk profile. They are much too vague and fail to mention the steps that are needed in between, which is probably why we face the current situation.

Basel II also makes it mandatory to choose one of three different approaches to further manage operational risks. These approaches are (in increasing order of prestige):

- The Basic Indicator Approach (BIA),
- The Standardized Approach (SA) and
- The Advanced Measurement Approach (AMA).

Each of these approaches has their own way of calculating the regulatory capital. The SA and the AMA also demands additional criteria to be satisfied before qualifying for these approaches. I assume that the reader is familiar with the basic differences between the methods, and will therefore proceed directly to explaining attributes that is directly correlated

with this thesis. Both the BIA and the SA approaches operational risk by establishing a capital that is based on the institution's income. Although this capital will be easy to communicate throughout the organization, it uses an extremely poor KRI for calculations. Income is not directly correlated with most operational risks, which makes the capital more esthetical than practical. In addition, there are no strict criteria, needed for qualifying, which could actively help the institution to control and communicate their risk profile. All in all this means that, except for a vague statement in Basel's principles for sound practice, there are currently none of these approaches that suggests incentives for properly measuring and communicating the risk profiles.

The AMA lets the organization estimate its own loss distribution, and further regulatory capital, by using a self-developed model. The only requirement when developing this model is that it should contain a mix of external and internal data, scenario analyses and business environmental and internal control factors (BEICF). Most of the current models focus on using mostly objective input like internal/external data, but some are also dominated by data derived from expert opinions on scenario analyses and the BEICF. In addition, the AMA also demands that the operational risk framework should be tied up with the daily risk management. This means that AMA currently facilitate the controlling and measurement of operational risks, which further enables the prospect of achieving the benefits of the dream scenario. The incentives that Basel II facilitates will be further reviewed and discussed in part three. Next, I will present the techniques that are currently being used for measuring individual operational risks.

1.3.2 Measuring and expressing operational risk

Market- and credit risk management has been measured and perfected since the dawn of the banking business. Most of the models that are used rely on quantified data, and may only include a small level of qualitative data, if any. This is mostly due to the access to huge databases of valid data which is deemed representative due to the law of large numbers. Operational risks rarely have these huge amounts of valid data. Consequently, it is preferable by most organizations to state it in a qualitative way by using words such as "low" and "high". This practice has led to many misunderstandings and ambiguity, and is probably the main factor why there recently has been an increased focus on quantitative statements. These methods are currently rather basic, such as the most common technique which is the *risk map* (see Figure 1.1).

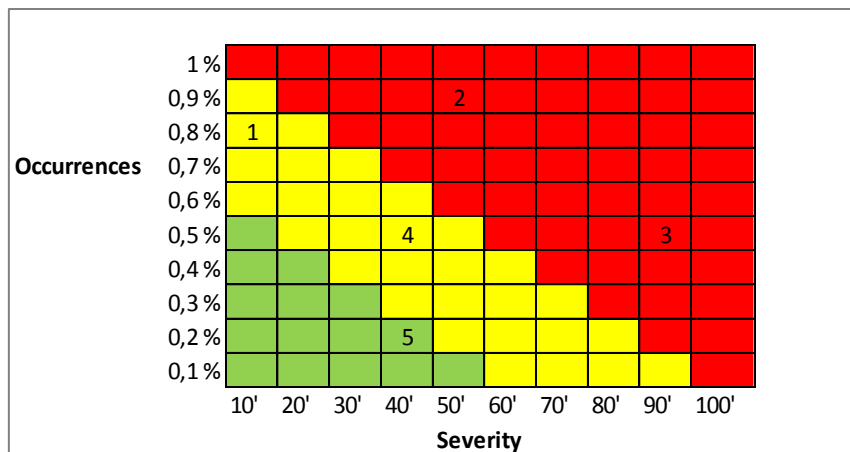


Figure 1.1 - Risk Map

The map itself is divided into several zones (often three) that explain the “danger-level” of the risk. These zones are most often color-coded where you have green, which is “safe”, red which is “dangerous” and shades between these two colors, like yellow and amber, to describe “warning areas”. In the case of this map (Figure 1.1), there are currently two risks (risk 2 and 3) that immediately have to be reduced (red zone), two risks (risk 1 and 4) that have to be managed and reduced over time (yellow zone) and one risk (risk 5) which currently is good (green zone). There is also a question of metrics when creating risk maps. This risk map uses a probability given as percent, and a severity in amounts, but many organizations choose to replace the amount and/or the percentage with points instead. This may be less work-demanding when assessing the risk, but it may also be a source of ambiguity.

The decision of where to place the risk may come from different sources, but usually it comes from the manager of the department that “contains” the risk. If the risk is spread over several departments, which would involve numerous managers, a weighted average could help to settle where the risk is placed. Risk maps may look different depending on usage, but the principle behind it is always the same. A closer review of risk-maps and alternative customizations to the use of it will be presented later in the thesis. This chapter only aims to present the reader with the current state and use of the technique. Next, I will present a survey on the use of risk appetite by the risk management in Norwegian banks.

1.4 Survey on the use of Risk Appetite in Norwegian Banks

The survey was conducted in order to get a better view perspective on how banks in Norway express their risk profile, with the assumption that risk appetite and risk tolerance are currently the most used terms when doing this. By using a website (Norges Største Bedrifter, 2011), I found the 100 biggest banks (rated by capital) in Norway. I chose to only include the 25 largest, which I found representative for my segment; “banks in Norway that *should* practice operational risk management beyond the regulatory boundaries.” Since both Husbanken (#4) and Statens Lånekasse (#5) are public institutions with goals of social surplus instead of financial profits, I chose to exclude them from the survey. This left me with 23 banks which gave a response rate of 96% (22 out of 23).

The respondents within the organizations were the managers of operational risk management. Depending on the size of the banks, the title of the respondents varied between Operational Risk Managers, Risk Managers and Financial-/Economic Officers.

1.4.1 What I wanted to find out

The following list will briefly explain the objectives of the survey:

1. How do the respondents perceive risk appetite and risk tolerance, both as individual terms and relative to each other?
2. How often are the terms “risk appetite” and “risk tolerance” used officially by Norwegian banks?
3. How are operational risks measured within the organizations?
4. Which barriers are perceived as the biggest when operationalizing a risk-statement?

In line with the rest of this thesis, my approach with the survey was to “scour the terrain”, analyze the results and see if there were any inconsistencies, which I in such a case, would point out and suggest improvements for. The foundation of existing data on the use of risk appetite in Norwegian banks are publicly non-existent which made it necessary to create an explorative survey to get more specific information. To see more detailed information of the questionnaire and the data please consult the appendix (Appendix 2).

The survey is originally in Norwegian, but the discussions of the result will be held in English, in line with the rest of my thesis. I will do my best to translate the information in an un-biased way, but the original report in Norwegian is in the appendix (Appendix 3) if there should be any doubt. I would also recommend any Norwegian readers to review the

mentioned report before reading the analysis to better grasp the essence of what is going to be reviewed.

1.4.2 Survey analysis and findings

The survey granted highly interesting results. I have chosen to divide the answers into four separate categories.

1. The first section includes the four first survey questions of the survey. These survey questions are closely related to the risk managers' individual perceptions and will answer the first stated question.
2. The second section contains survey questions five through ten. These survey questions focus on the organizations general strategies which should answer my second stated question.
3. The third section is focused on the measurement of operational risk which should answer my third stated question. The section consists of survey questions eleven through fifteen.
4. The final section consists only of survey question sixteen, which corresponds to the fourth stated question.

How do the respondents perceive risk appetite and risk tolerance, both as individual terms and relative to each other?

The first important observation came in the first question, and confirmed the belief that the current terminology suffers from ambiguity. Figure 1.2 shows a graph from the first question which clearly visualizes how differently risk appetite and risk tolerance are perceived among the respondents.

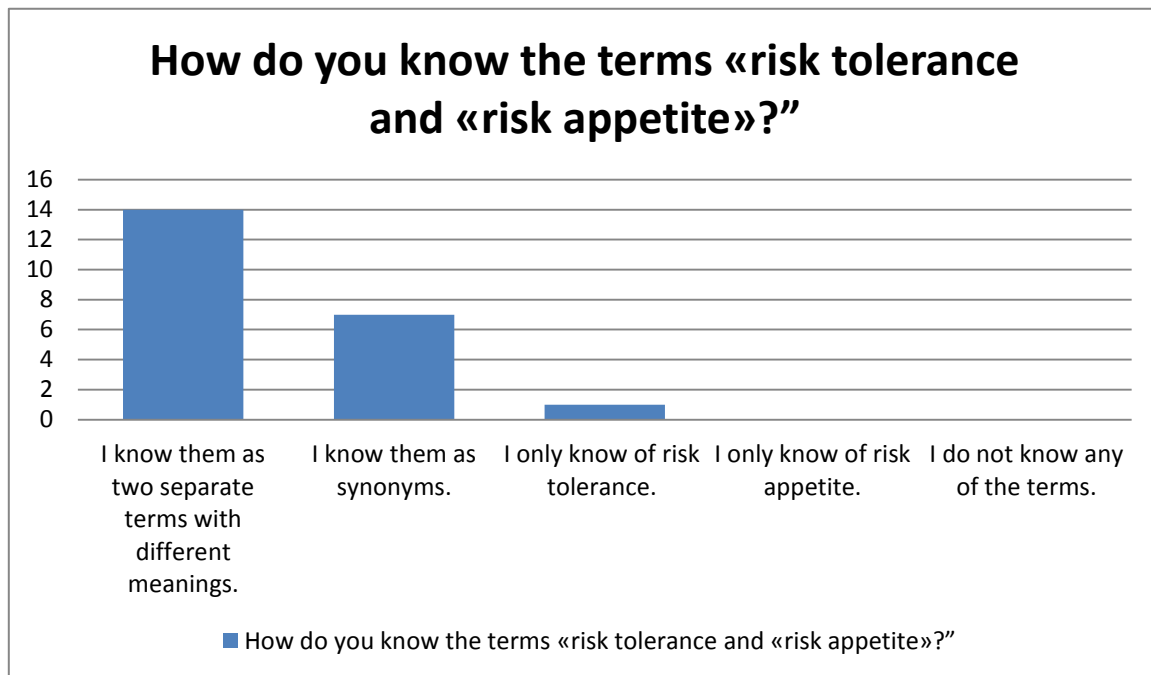


Figure 1.2 – How do you know the terms «risk tolerance and «risk appetite»?

Almost 2/3 see them as separate terms with different meanings, while almost 1/3 see them as synonyms. This further proves that Norway suffers from the same problem that was stated in Chapter 1.2.1, that there currently is no consensus on the terms in relation with each other. It is also important to observe that, with the exception of one respondent, all of the participants expressed that they knew about both of the terms.

After the respondents had explained if they knew the terms, they were further inquired to describe how they perceived these terms with their own words. This gave me a much deeper insight into the perceived opinions that the respondents had, which was perfect for the explorative purpose of the survey. The most interesting observation is that these two terms, that ideally should only have two perceptions, were perceived in five different ways. This is illustrated in Figure 1.3.

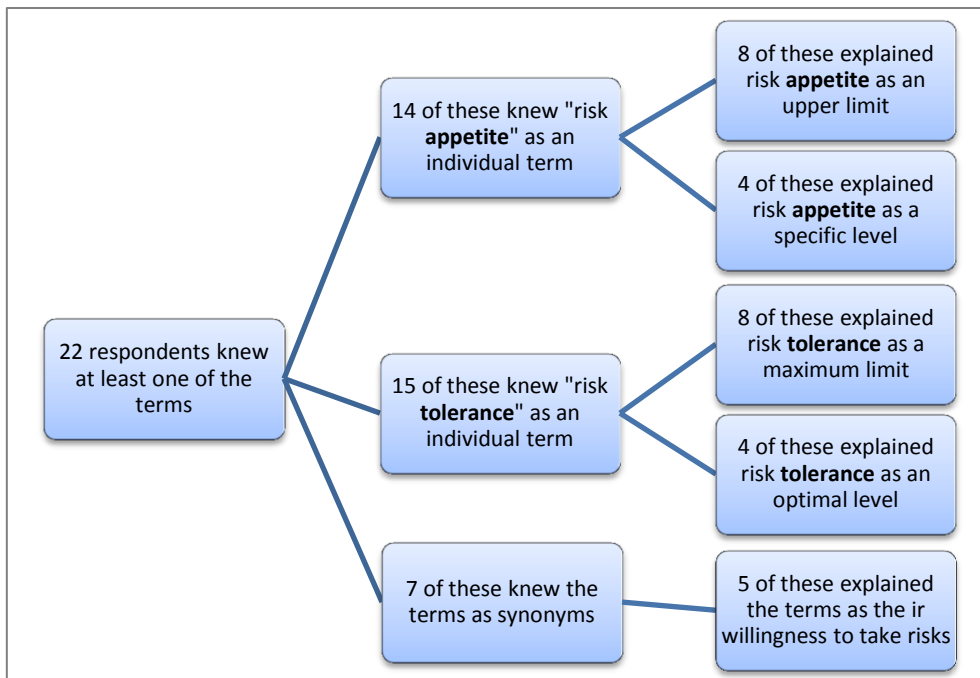


Figure 1.3 – Different perceptions of risk tolerance and risk appetite

The following section will go through these different perceptions in detail and explain them in closer detail.

Risk **appetite** as an upper limit

The first and most dominating category includes the respondents that expressed risk appetite as “*what they are willing to take*”. A total of seven respondents used a variant of the word “willingness” in their response. Another respondent with a quite comprehensive answer mentioned risk appetite as an: “*...acceptable risk relative to the organizations exposure...*” I have chosen to include all of these eight responses in the same group. I perceive this group’s answer in a way that they all understand risk appetite to be a term that explains “*The maximum limit of risk that the board wants to expose the bank to*”. This implies that the risk appetite sets an upper limit for risk exposure, not a lower limit.

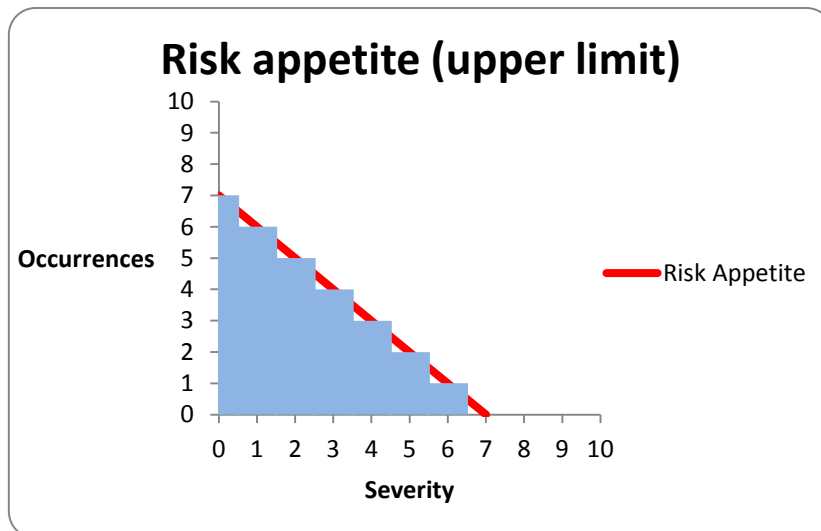


Figure 1.4 - Risk appetite as a maximum limit

As illustrated in Figure 1.4, any risks that are considered lower than the set risk appetite (within the blue area) would be approved.

Risk **appetite** as a specific level

The second group consists of the respondents that expressed risk appetite as something that they “wanted” or “wished” to take. Four respondents could be categorized into this group. I perceive this group’s expression of risk appetite as a term that explains “*The exact level of risk that the board wants to expose the bank to*”. By this I mean that the board has a specific level of risk that will set the risk exposure at a certain level.

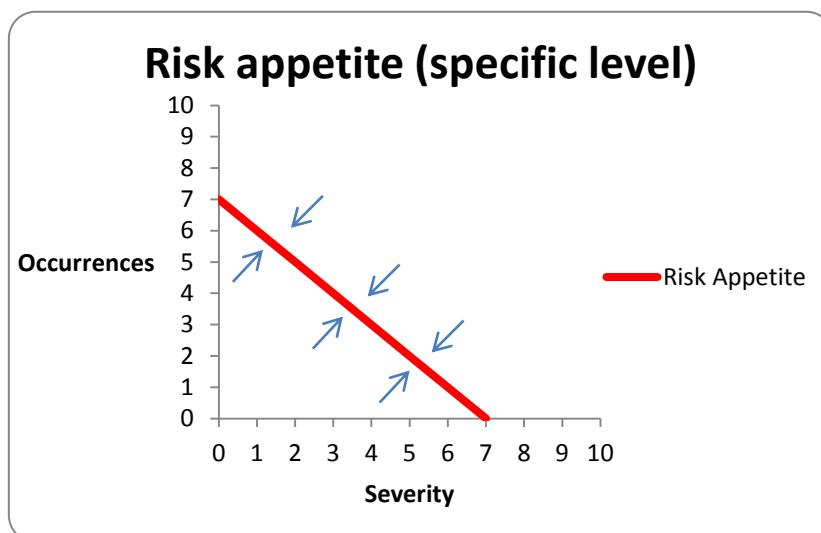


Figure 1.5 - Risk appetite as a specific level

As illustrated in Figure 1.5, a risk that are considered higher than the risk appetite level would be reduced until it is at the set level. Risks that are considered lower than the risk appetite

would, in the same way, be increased to the set level. This perception of the term is the most beneficial regarding to maximizing the control over the risk profile and minimizing the probability of misunderstandings through communication.

Risk tolerance as a maximum limit

The most dominating perception of risk tolerance, with eight responses, explained it with either “*endure*” or “*withstand*”. I perceive their explanations as risk tolerance being “*the maximum limit of risk that the bank can withstand*”. This means that if the estimated losses of the risk had increased, the bank would find itself in financial distress. For an illustration see Figure 1.6.

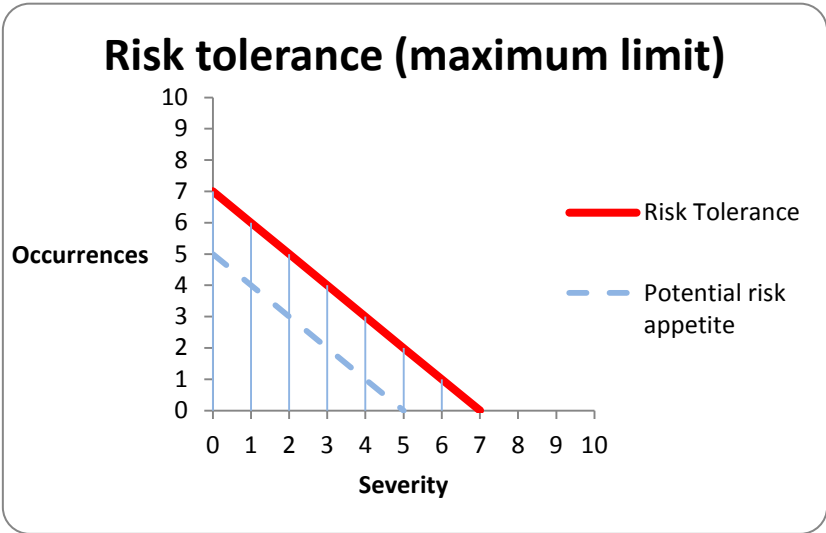


Figure 1.6 - Risk tolerance as a maximum limit

All risks that remain within the blue striped lines will not give any severe consequences, but the ones on the other side of the red line will send the bank into financial distress. I have drawn a potential risk appetite within the “safe zone” in order to not confuse this illustration with Figure 1.4. Another reason why the potential risk appetite is drawn is because some of the respondents mentioned risk tolerance as being the maximum limit of risk appetite. This seems like the most intuitive way to comprehend risk tolerance, which is a key property for poorly defined terms.

Risk **tolerance** as an optimal level

The second group consisted of four respondents and explained risk tolerance with words such as “*acceptable*” and “*necessary*”. The definition that I can perceive from these answers is that risk tolerance is “*a necessary limit of risk that a bank takes on and the acceptable limit that it operates at*”. This is illustrated in Figure 1.7.

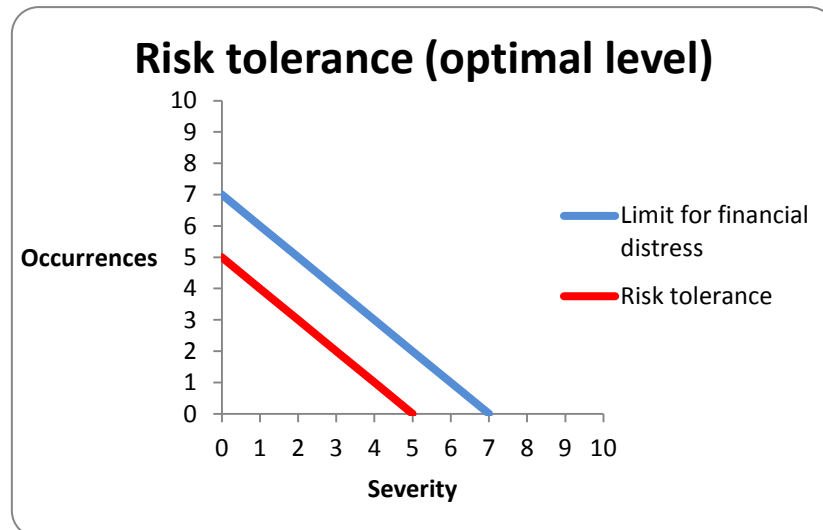


Figure 1.7 - Risk tolerance as an optimal level

In this case, the risk tolerance displays the optimal way of operating in an industry where risk is only considered negative, and should be reduced until the marginal benefits and costs of reducing the risk equals each other. However, this last conception of risk tolerance does not make much sense, and I must admit that I find it rather confusing.

Risk appetite and risk tolerance as synonyms

Out of the 22 respondents, seven perceived risk appetite and risk tolerance to be synonymic terms. Most of the seven respondents (five) that expressed risk appetite and risk tolerance as synonyms explained the term as the “*organization’s willingness to undertake risk*”. This is quite similar to the first of the risk appetite perceptions that was illustrated in Figure 1.4.

It is clear that the perception of these terms is much more differentiated than they should be. The problem with ambiguity is not only international, but very much present in Norway as well. This survey illuminates that two terms are almost evenly perceived in five different ways within the industry. This proves that something drastic needs to be done about it. An interesting extension to this research would be to further investigate if the perception of these terms were as varied within each organization as they are in the industry.

How often are the terms "risk appetite" and "risk tolerance" used officially by Norwegian banks?

To answer this question, it is important to both investigate how often the terms are being used on a daily basis within the banks, as well as how much they are used in official documents, such as a risk strategy. The answer to the first part of the question can be observed from Figure 1.8.

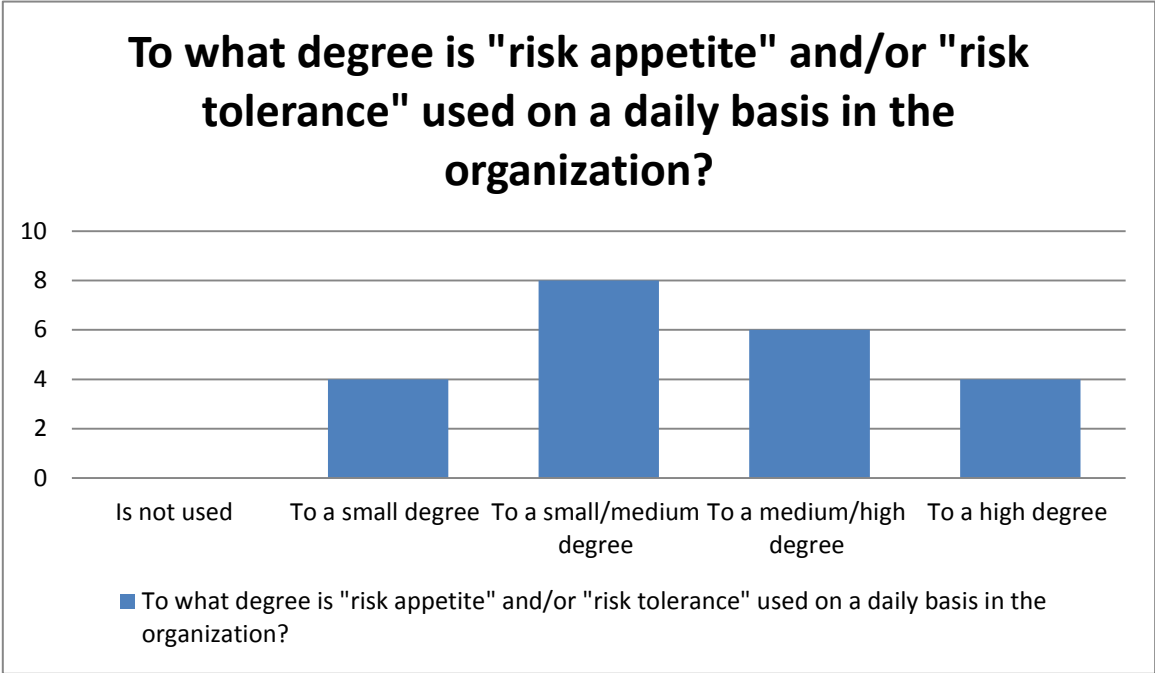


Figure 1.8 - To what degree is "risk appetite" and/or "risk tolerance" used on a daily basis in the organization?

This graph is from question five in the survey and shows that these terms are currently being used to a medium degree on a daily basis. A medium use of the terms within a company would qualify as a valid reason to continue this research, but let us first see if these terms are being used in the organizations risk strategies. Two questions inquired if the organizations had their own risk strategy, and which risks these strategies covered. All of the respondents expressed that they had a risk strategy, and 82% of these also stated that the risk strategy covered operational risks. Consequently, there is a good basis to assume that the next question also will be representative for operational risk strategies.

Figure 1.9 answers the second part of the question by showing if and how the two terms are being used in the risk strategies. I have added a cumulative bar to represent the three first yes-answers which makes the comparison between *yes* and *no* simpler.

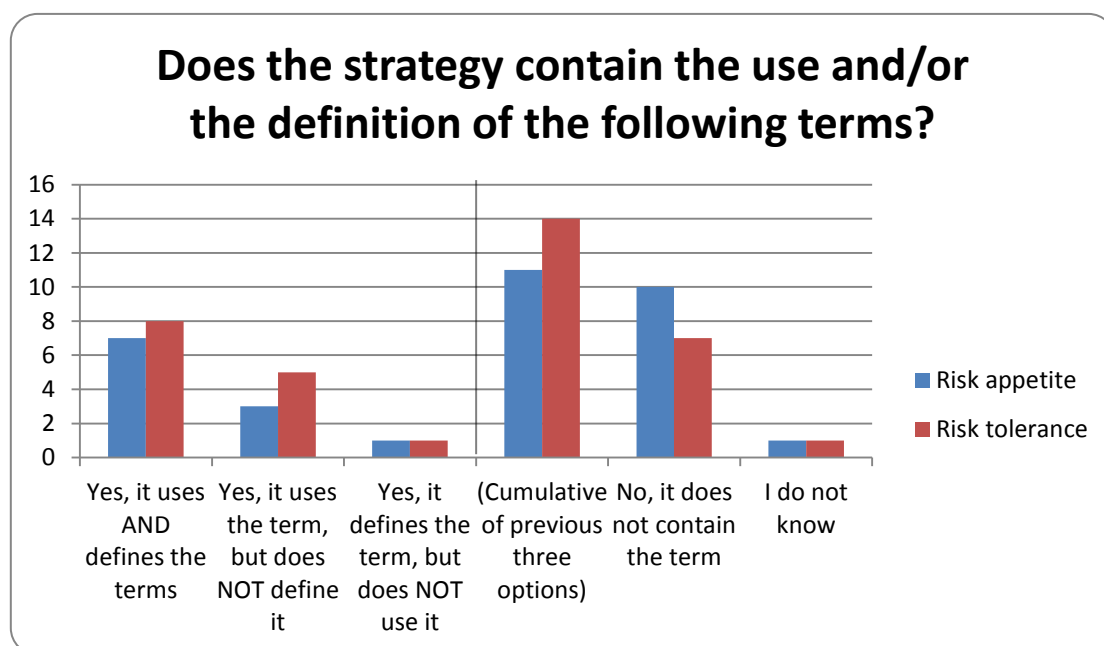


Figure 1.9 – How risk appetite and tolerance are used in strategies

There are two very interesting discoveries that can be drawn from this graph. The first one is that out of the organizations that use risk appetite, 73% have defined it, while only 64% out of the organizations that uses risk tolerance has done the same. The other interesting discovery comes from the comparison between the cumulative graphs of the banks that use and/or defines the terms and the banks that do not. This comparison basically creates a more detailed and official version of Figure 1.8 which reflected the use on a daily basis. There is almost a 50/50 split between banks that use and don't use risk appetite (respectively eleven and ten banks). Risk tolerance is clearly the most used term for expressing risk profiles with 64% of the respondents using it in their risk strategy.

The fact that 73% of the organizations that use risk appetite are able to define it, is definitely a good thing. My expectations were that it would be much less; and especially lower than risk tolerance. Only 64% of the organizations that use risk tolerance in their risk strategy are able to define it. This is quite disturbing, particularly when seeing how different the perceptions in the first question were. It is ensuring to see that almost three out of four banks define risk appetite, but the problems with ambiguity may not have existed at all if the banks had properly defined their terminology before actively using it.

I also took the opportunity to ask two questions about how the Norwegian banks were using these terms as well. These questions had some design-flaws (fully explained in Appendix 2)

which may slightly have biased the results, but I still think that they are relevant and worth including. The respondents had to choose if they expressed their risk profile quantitatively, qualitatively or in other ways. Most people expressed that they used both methods which is why I have adjusted the graph to reflect this (Figure 1.10).

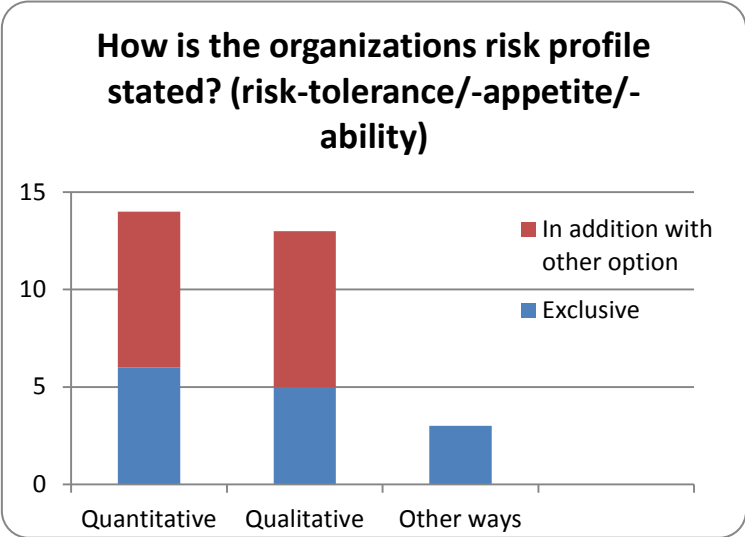


Figure 1.10 – How organizations’ risk profile is expressed

The red bar represents eight banks which uses, both, quantitative and qualitative methods, while the blue bars are the banks that only use quantitative or qualitative (respectively six and five banks). Due to the design-flaw only eight respondents were inquired if they measure operational risks in a quantitative way as well. Only 25% answered “Yes” to this, which is quite low and may indicate a source for miscommunication.

It is positive to see that most of the banks actually combine both quantitative and qualitative objectives. A qualitative statement usually offers a larger context, which helps the reader to understand any unclear terms through the context, while quantitative statements are much more precise and easier to communicate, as long as you understand the terminology that is used. The probability of misunderstandings is reduced when quantitative and qualitative statements are combined, which is a good thing. However, I believe that the results show that the organizations only use qualitative statements where they find it impossible to use quantitative metrics. This would indicate that they are used exclusively and not combined, which is quite disturbing.

How are operational risks measured within the organizations?

The survey approached this section by asking two questions; if the responding organizations currently had a clear and documented strategy for operational risk, and to what degree this strategy was operationalized. If none of the participating organizations had operational risk strategies, it would not be likely that they actively measured or managed their operational risks either. A graph which displays both of these survey-questions can be seen in Figure 1.11.



Figure 1.11 – Operational risk-strategies in Norwegian banks

As we can see from the figure, it is increasingly more common to have a specified risk-strategy within operational risk management. Since only approximately half of the banks that have started the process have fully operationalized their strategy, it shows us that this is a highly relevant subject, and that many would benefit from the research done within this field.

This section's main purpose, however, was to find out how individual operational risks were measured, which was done through two additional survey questions. The first of these two questions asked; how many operational risks has the bank identified? The results are in the following table (Figure 1.12):

| Alternatives | Response (Percentage) | Response (Value) |
|--------------------------------|-----------------------|------------------|
| Over 50 risks | 13,6% | 3 |
| 10-50 risks | 54,5% | 12 |
| Under 10 risks | 4,5% | 1 |
| It is not identified any risks | 9,1% | 2 |
| Other | 18,2% | 4 |

Figure 1.12 – How many operational risks have Norwegian banks identified?

We can easily see that most banks identify between 10 and 50 operational risks, which is quite good. The ones that answered “other”, states that they identifies risks, but that they do not have the amount of risks identified in front of them. This means that actually 90,9% of the responding banks measure one or more operational risks. The survey then further inquired whether these individual risks were individually quantified, in which the answers can be seen in Figure 1.13:

| Alternatives | Response (Percentage) | Response (Value) |
|-----------------|-----------------------|------------------|
| Yes, as points | 37,5% | 6 |
| Yes, as amounts | 6,3% | 1 |
| No | 43,8% | 7 |
| Other | 12,5% | 2 |

Figure 1.13 – Are the identified risks quantified?

Most of the respondents that was asked this question did not quantify their operational risks on an individual level. Among the ones that did measure the risks individually, there seem to be a tendency towards measuring with points instead of amounts. One of the respondents that answered with the “other”-alternative stated that they try to use amounts in all possible cases, but that it is sometimes impossible.

Which barriers are perceived as the biggest when operationalizing a risk-statement?

This section is only covered by a free-text question which asked: “What do you see as the biggest barrier to become better at implementing the board’s expressed risk-level into the daily risk management?” This is a rather complex question which also is reflected in the huge variety of answers from the respondents. Through the first part of the thesis I have explained the reasons why organizations currently cannot communicate and control their risk profile properly from a theoretical viewpoint, but this question lets us take look at what the organizations themselves see as the biggest barriers.

Most of the respondents’ answers mention that communication related issues are the biggest concern. This is very much consistent with my theoretical conclusions from both Chapter 1.2

and 1.3; the risk terminology is currently too ambiguous and the metrics, as well as the measurement techniques, is not very communication-friendly. It is therefore not surprising that the two other recurring answers are *problems with understanding the risk profile* and *measuring and/or quantifying operational risks*. These answers stresses the importance of the main arguments in Part one of the thesis: Something drastic needs to be done.

1.5 Conclusion

Part one of this thesis has reviewed the current state of how organizations are expressing and managing their risk profiles. The findings from the survey illuminates that it is still a long way to go until a perfected process for this is developed, and it seems that the development currently has reached an impasse. Risk appetite has been the most frequently used term by organizations to express their risk profile, but Chapter 1.2 proves that this term is currently too ambiguous to be used for anything. Chapter 1.3 also proves that risk appetite may not be the only source behind the communicational problems. The current measurement techniques, as well as the parameters used by organizations are currently much too counter-productive regarding communication, and should be properly assessed for improvements. The survey in Chapter 1.4 further proves both of these theories and also adds risk tolerance to the list of ambiguous terms that explains a risk profile.

It may seem like this is a compilation of several different problems, but they actually boil down to two issues: The first issue would be to assess the current risk terminology and improving it. To successfully communicate and control the risk profile, an organization would have to express two different risk-levels. The first one has to be the maximum risk-level that the organization has the ability to expose itself to without causing financial distress. The second risk-level should be the level that they prefer to be at. If organizations individually express, both, their maximum ability for risk and their preferred level of risk, they can create synergies that would severely improve both internal and external communication of the risk profile. This issue will be further assessed in part two of the thesis.

The second issue that needs attending is the problem of choosing proper metrics and techniques for measuring and stating individual risks. One of the biggest challenges is to find an optimal measurement technique that can help organizations away from using qualitative metrics and instead using quantitative metrics. This also includes finding a quantitative parameter which optimizes communication. The second issue will be assessed in the third part of the thesis.

Part II
- Improving the Risk Terminology -

2.1 Introduction

This part will further help the reader to understand and reflect more on the current problems that operational risk-terminology faces. As mentioned in part one, something drastic needs to be done in order to improve operational risk profiles. The definitions of risk appetite are currently much too ambiguous, which makes the term a poor candidate for expressing risk profiles. The conclusion from Part one of the thesis points towards trashing “risk appetite” as a term in the operational risk-terminology. The definitions are not the only source behind the terms ambiguity, and Chapter 2.2 will prove this by discussing the term’s literal meaning and its ethical implications.

Part one of the thesis, along with Chapter 2.2, ultimately concludes with dismissing “risk appetite”. This will leave a vacuum in its place that needs to be filled with clearer and more defined terms. As mentioned in Part one, organizations would benefit most by using two terms to express their risk profile; a term that reflects its maximum risk-limit and a term that reflects their preferred level of risk. The vacuum that risk appetite leaves is the perfect opportunity to apply this practice, which is exactly what this thesis will do. Chapter 2.3 will first take a closer look at the definitions of the discarded term, which is important in order to learn from the mistakes that made the term risk appetite useless. The chapter will then proceed with the search for alternative terms by exploring the petroleum industry’s operational risk-terminology. Finally, Chapter 2.3 will use the gathered information and select the best alternative terms to represent the new concept.

Chapter 2.4 will officially bring the formerly discussed concept into the world, and name it as RiskPAT. The chapter will start of by briefly presenting it, before getting into the technicalities. It will then continue to mention opportunities that can arise when using RiskPAT and some pitfalls that should be avoided.

Part two will be concluded in Chapter 2.5, which will summarize RiskPAT and explain how it may be the next big step towards perfectly communicating and controlling risk profiles.

2.2 Dismissing “Risk Appetite” from the Risk-Terminology

“Risk appetite” could probably have been sorted out as a term if the only problem with it was that it was poorly defined. Basel could have set their foot down and decided on one definition, or all the organizations that were using it could have attached a clear definition to every document where it was applied. The problem, however, is that the definitions are not the only source of ambiguity when it comes to risk appetite. The phrase “risk appetite” uses the word appetite, which in a cognitive way illustrates images of desire, natural needs and hunger. This is a clear contrast to the word “risk”, which is usually linked to something that is objective, quantified and calculated, basically a measure of the probability to reach a certain future state. When appetite for food arises, a cognitive response tells us that we should eat. There are no cognitive responses that naturally decide what risk is optimal for an organization. A preferred level of risk will only exist after thorough discussions among the stakeholders and heavy calculations. Put to the point; is it ethically sound to enforce the use of a term that encourages the treatment of risk in the same instinctive way as an everyday meal?

The ethical problems with using “appetite” may lie in the type of risk that it is applied to. In most financial risks there are upsides as well as downsides. In market risk, when buying stocks, the volatility will generally have an equal chance of either increase or decrease the stock’s value. Credit risk is mostly seen as a downside risk, but the risk you take on is often mirrored in the borrower’s interest rate, which makes a profit as long as the borrower manages to pay back. Both of these risks grants net profits if the company that takes them, manages to “beat the odds”. This will in other words mean that you earn on another organization’s fortune and/or mistakes. The word “appetite” may be valid for taking these risks on, since they may lead to a positive outcome which grants satisfaction and furthermore saturates your hunger for risk. This is not the case with operational risk.

Let us first discuss operational risk from a theoretical perspective which assumes that the world only takes decisions that are ethically sound. Operational risk is defined by Basel as “*the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events*” (Basel, 2001). Upsides that may come from this are extremely limited. A book by David Tatham states that there are only two possibilities for upsides in operational risk. The first one is if an employee accidentally places an order on 10.000 shares instead of 1.000 shares, and the profit that may arise in the increase of stock value from the time the shares are bought until the mistake is discovered and the excess shares are sold. The other one is in the event of an external event, such as a pandemic, arises, and it

leads to an increase in sales for a pharmaceutical company (Tattham, D, 2011). This is, however, a question of semantics since both examples could be divided into several risk types where e.g. employee error = operational risk and stock increase = market risk. Either way you see it, there are few to none benefits to gain from taking on additional operational risk from an ethical sound viewpoint. This is also the reason why “appetite” is confusing to use, and theoretically does not make any sense in an operational risk context.

This may, however, be perceived differently in the real world where ethicality is not presumed. There will always be some “rotten apples” in the financial industry who seeks to earn money on other peoples ignorance. In this case, operational risks do have the ability to yield profits. World Games Inc., Enron and Acta Kapitalforvaltning are all examples of businesses that have earned money by withholding vital information from their stakeholders. Let us take a closer look on Acta Kapitalforvaltning, a Norwegian brokerage firm which was convicted of illegal marketing of structured financial products. The marketing led to believe that the structured products was far less risky than they actually were, which made more people invest in them. This may have been highly unethical, but it still granted revenues and it fully due to explosion to an operational risk. Operational risk may not be profitable in a theoretical and ethical environment, but in the real world, ethical behavior is not necessarily given. Some un-ethical business cultures have found a way to earn money on keeping operational risks high. Whether or not this is a conscious action by the boards in these organizations is not for me to reflect upon. My only intension is to illuminate the fact that operational risk may also grant “upsides”. Even though, any financial organization would, most likely, never want to associate itself with un-ethical behavior, which further still means that “appetite” is an invalid word to use when expressing an operational risk profile.

In operational risk, “risk appetite” is a term that does not make any sense, because *risk* (from an ethical context) is exclusively regarded as negative, while *appetite* is defined by the dictionary as a strong desire for something. Why should we use a term that is contradictory to itself by definition? This discussion concludes that even the natural interpretation of the term “risk appetite” is a source of ambiguity, which further proves the need to dismiss the term from the operational risk-terminology. The next problem, which is to find two terms which are clear, concise and easily understood to fill the void that “risk appetite” leaves behind, will be assessed in the next chapter.

2.3 Searching for Alternative Terms

It is paramount to learn from the mistakes of the ambiguous definitions when finding new terms. The thesis would have been proved to be useless if the new terms should suffer from the same ambiguity that risk appetite suffered from. It is therefore crucial to analyze the flaws of the term “risk appetite” before the search for alternative terms can begin.

2.3.1 Learning from the mistakes of risk appetite

All the definitions in Chapter 1.2.1 try to state risk appetite in different ways, but none of them take other risk-terms, such as e.g. “risk tolerance”, into the definition so the reader can relate it to something. If risk appetite had been defined relative to another term, it could have decreased the terms ambiguity. To prove this, I will present an example where I use risk tolerance as a related term to risk appetite. To make the example more convenient, I will define “risk tolerance” as the ultimate level of risk that can be tolerated by a company before going into financial distress. If the level of risk exceeds this limit, the company would ultimately be bankrupt. Now that we have a level to relate to (risk tolerance), I will make three very plausible conclusions on what risk appetite is from the definitions in Chapter 1.2.1. Watch Figure 2.1 for an illustration.

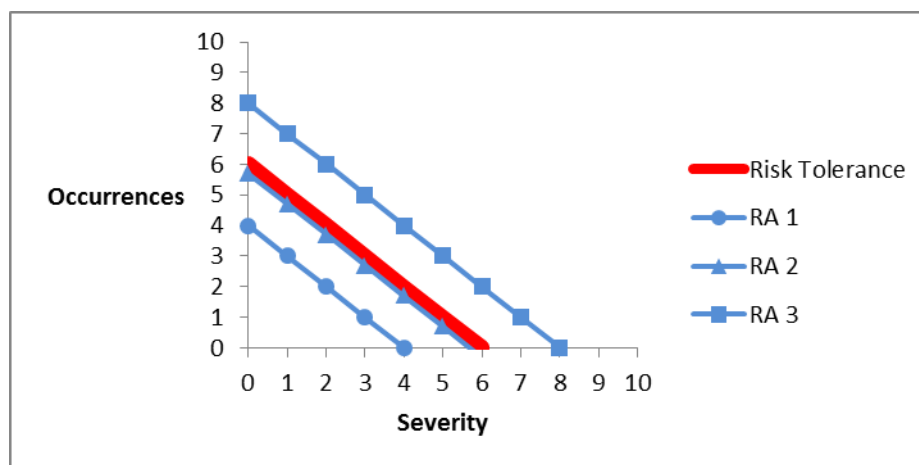


Figure 2.1 – Different plausible conceptions of the term “risk appetite”

The first plausible adaption of risk appetite is labeled **RA 1** in the figure. This is the level where the risk is at a very low level and where risk appetite is defined to be within the risk tolerance. This could very much be in tone with all of the found definitions since it could express the “...willingness to take on risk” from a person that perceives risk appetite to be a narrower term than risk tolerance. If this is the local perception of the definition within the company, it would also be true that “It is the amount of risk that the organization is willing to accept in the pursuit of future objectives”.

In **RA 2**, risk appetite and risk tolerance has become synonyms instead of being relative to each other. This could also be justified as a plausible belief since the definitions only state *willingness* as mainly being the only objective that needs to be fulfilled, and British Standards even mentions it as being “...[what an organization] is prepared to seek, accept or tolerate.”

The last way of perceiving the term is illustrated by **RA 3**, where the risk appetite is way above the risk tolerance of the organization. The government often has to apply several limitations on banks so that they do not risk bankruptcy. The only reason that this needs to be done, is because the banks may have a larger appetite for risk than what is optimal for them. It is only in this belief of the term that the word *appetite*, as earlier discussed, really fits in. The only definition that counters this belief is British Standards (BS), which limits the risk appetite to be what an organization can *tolerate*. In this case the risk is clearly out of the bounds of risk tolerance, which does not comply with BS. It is, however, still interesting to mention it due to the adaption of *appetite* in a literal sense.

The definitions of risk appetite have generally been too vague to really prove or disapprove various perceptions of the term as proven in this example. An important lesson to learn from this is to only use brief, clear and concise definitions of the new terms. It is also crucial to find terms that will contain words that are very natural, adaptable and ethical when used in a risk perspective. The petroleum industry is a pioneer when it comes to managing operational risks, and also fits as the perfect starting point in the search for these two new terms.

2.3.2 Controlling risk profiles in the petroleum industry

The petroleum industry has always been innovative with operational risk research, which is also the case when it comes to creating tools and concepts that limits and controls risk profiles. It is important to think of the differences between the petroleum- and the bank-industry if terms should be transferred from one industry to another, but this will be discussed more thoroughly later. When it comes to available material on the subject of operational risk-terminology in the petroleum industry, there is plenty to choose from. Most of this sub-chapter will be based on information gathered from the book “*Risk Management: With applications from the Offshore Petroleum Industry*”, which is written by Terje Aven and Jan Erik Vinnem (Aven and Vinnem. 2007).

Risk acceptance criteria

Risk acceptance is the most common term within the petroleum industry for stating and/or limiting the risk profile. The risk acceptance criteria has been the most used method for

limiting risk on the Norwegian continental shelf. Similar to the ideas of the “risk appetite-statement”, one finds a criterion that is relevant for the specific risk and then sets an appropriate limit on it so the risk is kept within an acceptable level. I have illustrated this in Figure 2.2.

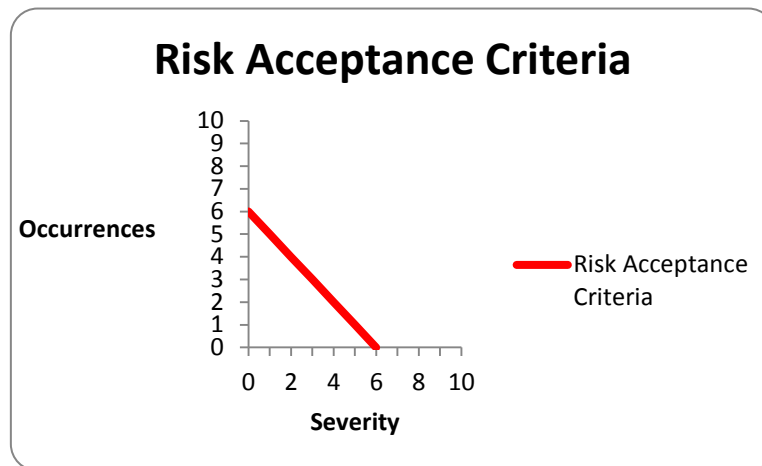


Figure 2.2 – Risk Acceptance Criteria

The idea behind it is simple and logical; if the risk is judged to be outside its limits, it is not acceptable and must be assessed. There are, however, some valid arguments against this process. Aven and Vinnem points out these two points:

- “1. The introduction of pre-determined criteria may give the wrong focus – meeting these criteria rather than obtaining overall good and cost-effective solutions and measures.
2. The risk analyses – the tools used to check whether the criteria are met – are not generally sufficiently accurate to permit such a mechanical use of criteria.”

(Aven and Vinnem. 2007)

It is pleasant for the state of mind to have a border that either states the risk as *negligible* or *intolerable*, but risk should not be “pleasant for the mind”. Down-side risks are something that should be as low as possible, and a border that gives a green or a red light will only decrease the innovativeness of risk-reducing measures. There is little value that can be retrieved from the risk acceptance criteria, but there may be something to learn from the next method which is known as ALARP.

ALARP

The ALARP (As Low As Reasonably Practicable) principle encourages a continuous improvement risks. An ALARP assessment consists of three regions:

1. The region is so low that it is considered negligible.

2. *The risk is so high that it is intolerable.*
3. *An intermediate level where the ALARP principle applies.*

(Aven and Vinnem. 2007)

The ALARP is illustrated in Figure 2.3.

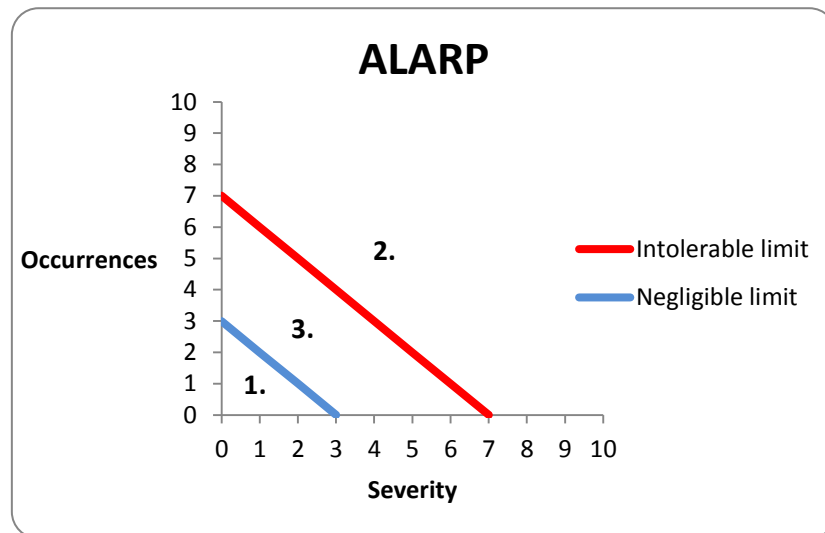


Figure 2.3 - ALARP

The thought behind this idea is for the authorities to inspire organizations to continuously improve its risk management as long as it is reasonably practicable. If a risk is considered to be within region 1, it would mean that the risk should be considered negligible, and do not need any assessment. This limit is strictly set, so to see a risk beneath this threshold is uncommon. If a risk is in region 2, it is regarded as intolerable. This means that the organization either needs to abandon the risky activity or implement risk-reducing measures immediately. The risk must at least be brought within region 3 to be accepted. Region 3 is the ALARP-region. When a risk is within this region it is in a state of continuous improvement. The ALARP principle states that any countermeasures to risk shall be implemented as long as the cost is not grossly disproportionate to the benefits. In practice this means that any organization with risks within this region needs to document any countermeasures that they may think of, and then either implement them or give a well-documented reason as to why the costs are seen as “grossly disproportionate” to the benefits. Some aspects of the ALARP have already been introduced to the financial industry through risk maps, but there may still be more that can be learned in terms of strictness and its use of real amounts.

It is, as earlier mentioned, crucial to be aware of the differences between the oil industry and the financial industry when transferring knowledge between them. The main difference

between these industries when it comes to operational risk management is that the petroleum industry is much more about safety for the employees than making money. In the bank industry, one might risk to lose a million dollars, while in the offshore industry the risk may be to lose the life of an employee. This implies that the petroleum industry most likely have developed risk management tools which emphasize the minimization of risks, while the financial industry would be more interested in tools that emphasize control of risks. It may be beneficial to find inspiration in other industries, but when it comes to finding new terms I have found that the best solution is to do it on my own.

2.3.3 Revealing the new terms

Through my search for the new terms I have stated that I wanted to find simple and naturally adaptive terms. Since the first term should explain the organizations preferred risk profile, I have chosen to simply go with the term *risk preference*. Risk preference is a very intuitive term, which makes it easier to avoid miscommunication, and is also ethically proof. By using risk preference, one simply states that it is the risk profile that organization prefers to have. The risk preference could technically be set at any limit. Some boards might prefer a higher risk exposure than their organization is limited to, while others might want to mitigate their risk exposure and therefore prefers to stay beneath their limits.

The limits which are mentioned in the end of the last paragraph are the limits that are set by the second term. This term is meant to explain the maximum limit of risk that the organization can take without going into financial distress. It was a close race between *risk ability* and *risk tolerance* when deciding this, but I decided that *risk tolerance* was the best term since it properly reflects that this limit should not be bypassed. Risk tolerance is, in the same way as risk preference, also an intuitive and ethical sound term which can easily be understood as *the risk that the organization tolerates*. Risk tolerance is already a well-established term, and should be the most intuitive term to use. The survey showed that there were some ambiguity with the term, but I think this could be solved by expressing it clearer through a context. Risk tolerance also works as a perfect term to explain the upper limit which the organization needs to stay within to avoid financial distress. The next chapter will discuss this more thoroughly and present the concept which uses risk preference and risk tolerance in collaboration with each other to improve organizations communication of risk profiles.

2.4 RiskPAT: A New Concept for Managing Risk Profiles

Risk appetite did not have the properties to solve the problem of communicating and managing risk profiles, thus I have developed RiskPAT. RiskPAT stands for Risk – preference/-acceptance/-tolerance, and will significantly improve the possibilities of controlling, managing and communicating an organization’s risk profile. The observant reader might wonder why *risk acceptance* is included in the abbreviation, which is a question that will be answered in Chapter 2.3.4. *Risk acceptance* can therefore be ignored until then.

2.4.1 Brief preview of RiskPAT

RiskPAT is a basic concept which uses two terms; “risk preference” and “risk tolerance”, in collaboration to create synergies. We have seen throughout this thesis that confusion easily can arise around long and complex definitions, which is why I chose to emphasize on finding the most natural and understandable terms.

To properly communicate the risk profile to both internal and external stakeholders, they will need to know three things:

1. The risk profile that the board *want* the organization to have (exact risk level).
2. The risk profile that the organization *needs* to be held within to avoid financial distress (upper limit).
3. The one risk profile, out of the previous two, that they can expect the company to be at.

By applying risk preference to number one and risk tolerance to number two we have all the terms in order to express the risk profile in the best possible way. After an organization identifies their risk preference and their risk tolerance, they can easily see which of the two that is the most rigorous. The strictest one of the two terms will always be the level of risk that the stakeholders can expect the organization to be at, which would be the third, and last, point on the list of things the stakeholder should need to know about the risk profile. By knowing these three values about the risk profile, one would get a better and more understandable insight into what the board wants for the company. See Figure 2.4 for an illustration of the concept.



Figure 2.4 – The concept of RiskPAT

Now that the concept of RiskPAT has briefly been presented, the thesis will continue to present the technicalities behind it. The next sub-chapter will start with explaining what each of the terms contributes with.

2.4.2 The contribution of each term

The risk that the board wants to take

It is important to inform the stakeholders of what risk the board wants to take if it was on a “looser leash” than the surrounding environment actually allows. The best term to express the risk profile that the board *wants* is risk preference. It is essential that the set level of the risk preference is exact and expressed as a target, not as an upper limit. This is because the risk preference is a preference, not a limit, and preferences cuts both ways. No bank would accept it if a department chose zero risk, even if they are within the risk preference. A bank’s core business is, after all, to create value by taking and controlling risks and that can only be expressed by setting the risk preference as a specific value.

The risk that the organization is limited to

The second term is equally essential for communicating the risk profile in a proper way. It represents the limit created by regulatory commitments, market fluctuations, rating bureaus and other surrounding influences, which the organizations are forced to keep within to avoid financial distress. The term which fits best for this maximum limit of risk is “risk tolerance”. To tolerate something is defined as: “*To allow the existence, presence, practice, or act of without prohibition or hindrance; permit. (Dictionary.com, 2012)*”, and this is exactly how tolerance should be interpreted in this context as well. By now, many of you might think that

this is exactly the same as risk preference, but it is not. While risk preference represents an internal set limit, the risk tolerance is the limit that is tolerated by the external world. It explains how much risk the external environments, such as the government and rating bureaus, are indirectly allowing the organization to take. This is, naturally, expressed as a maximum limit.

The lowest limit of the previous two

One of the two previously mentioned limits will always be lower than the other one. In some few cases, the surrounding influences will cause the banks to have a stricter risk tolerance than their risk preference, while in most cases banks will choose a risk preference beneath the risk tolerance and thereby take less risk than the surrounding influences restrict them to. The lowest one of these two limits will consequently always be the best estimation of the *true* risk profile, since it is the only possible level of risk that the organization can optimize its operations, at when regarding both external and internal views. The next sub-chapter will take a closer look on how RiskPAT would work in a real world setting.

2.4.3 Applying the new concept

RiskPAT may be exposed to many different ratios between risk preference and risk tolerance. This sub-chapter will cover the theoretical variations that the concept might face, which will further prove RiskPAT's adaptability as well as the positive effect it has on the organization. Two examples will be presented with the use of RiskPAT within the field of operational risk. The examples will, respectively, be about banks that have low and high risk preferences. It is, however, necessary to take a closer look on the RiskPAT's dynamics before presenting these examples.

The dynamics of RiskPAT

RiskPAT is designed, as earlier stated, to optimize the communication of risk profiles without ambiguity. By demanding that each organization states both their risk preference and their risk tolerance, an interested third-party (e.g. rating bureaus or investors) would receive all the information they need to know about the organization's risk profile. Firstly, they would know exactly at which level the risk profile would be at any time. This risk level will always be stated by the lower of the two terms, which is a result of the dynamic collaboration of the terms.

In cases when the *risk preference* is higher or equal to the *risk tolerance* it is expected by the RiskPAT that the true risk profile will be at the same level as the risk tolerance. In this

scenario the organization actually wants more than they can take. Thus, it is most likely that this specific organization would maximize its risk exposure to get as close to their risk preference as possible. This maximization would come to a halt at their risk tolerance since any organization, by definition, would significantly decrease its value and/or go bankrupt if they bypass this limit. The true risk profile would therefore in such cases equal the risk tolerance.

In cases when the *risk preference* is lower than the *risk tolerance* it would be expected by the RiskPAT that the true risk profile would equal the risk preference. In this scenario the organization prefers a profile that is more risk averse than the risk tolerance actually allows. This means that the organizations have the ability to achieve the profile they prefer without risking financial distress. This implies that the true risk profile in such cases would equal the risk preference.

The balance between the *risk preference* and the *risk tolerance* will also help a stakeholder to reveal the characteristic of the organization. A risk averse investor who is interested in long-term investments with a low and steady return, could now find the organizations that have a risk preference below their risk tolerance. This characteristic points out that the investor could still expect the organization to have the same true risk profile even if the risk tolerance should temporarily shift outwards.

Now that the dynamics of RiskPAT has been discussed I will move on to present the two previously mentioned examples.

Example 1: Low risk preference

The board at Bank A is relatively risk-averse and has recently expressed that they want to minimize their operational risk exposure. They know that there will be high costs associated with this process, but they figure it is worth it due to a “healthier” risk-image. The board signals this by stating their operational risk preference as low and adds a quantitative goal which states that the organizations operational risk should be at 3% below the minimum regulatory requirement at any time. They immediately start to work with adjusting their risks by reviewing their incentive programs and by implementing comprehensive control processes.

After a risk committee from Bank A has gone through the operational risks in the organization’s sub-divisions, they set specific goals for each division that are directly derived from the overall statement. Since the risk preference in this case is mentioned as relative to

one of the central factors of the risk tolerance (regulatory requirements), it might not come a as surprise to them that the preference is lower than the tolerance (see Figure 2.5). This would therefore make the risk preference equal the expected level of Bank A’s true risk profile.

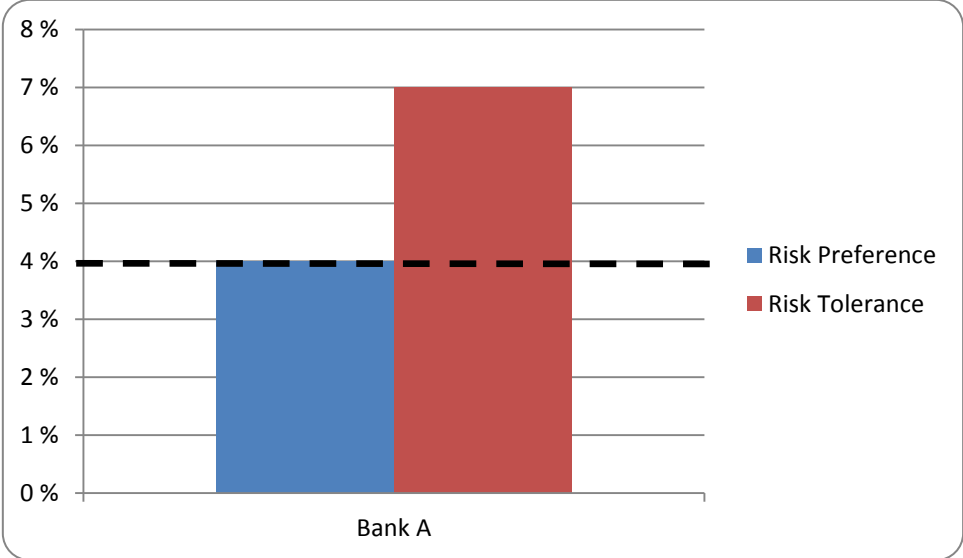


Figure 2.5 – Low risk preference/high risk tolerance

When the board has publicly stated both the risk preference and the risk tolerance of the organization, it will make it easier for future and present investors to know what to expect of the bank. Not only do they know which level of operational risk that the organization will revolve around, but they also know that this bank further restricts itself from what is necessary (*Preference < Tolerance*). This could, as earlier mentioned, be appealing to many long-term and risk-averse investors, which is further exactly the kind of investors that Bank A wants more of. The investors could also expect Bank A to most likely keep a steady operational risk profile as long as the risk tolerance is not lowered too much.

Example 2: High risk preference

Bank B is a risk-loving bank which seizes the opportunity to make money where they can. This is probably the case with all banks and organizations, but Bank B has a reputation for increasing their profit by operating in certain gray-areas. It only hires the “best of the best”, has a high turnover-rate and the culture is highly focused towards profits and aggressive incentives. This makes the bank’s risk preference relatively high, a fact that Bank B wants to state publicly, since it may attract investors with the same risk-seeking attitude to their organization. The board states that they have a high risk preference for most risk types, also including operational risk. They know they can exploit some un-ethical “upsides” of

operational risk and states a quantitative risk preference to be at 10% of the organization’s profits.

The board appoints a risk committee which becomes responsible for measuring the current level of operational risk within the organization, and the level of operational risk tolerance that the bank is restricted to. After measuring the risk within all of the sub-units they find optimal KRIs for measuring the risk within each sub-unit. In addition, they also look at the regulatory requirements and other external effects that regulate the risk tolerance. They quickly find that the risk tolerance is stricter than the set risk preference, which limits the amount of operational risk to be held within the risk tolerance. The risk tolerance will therefore be the estimated level of Bank B’s true risk profile (see Figure 2.6).

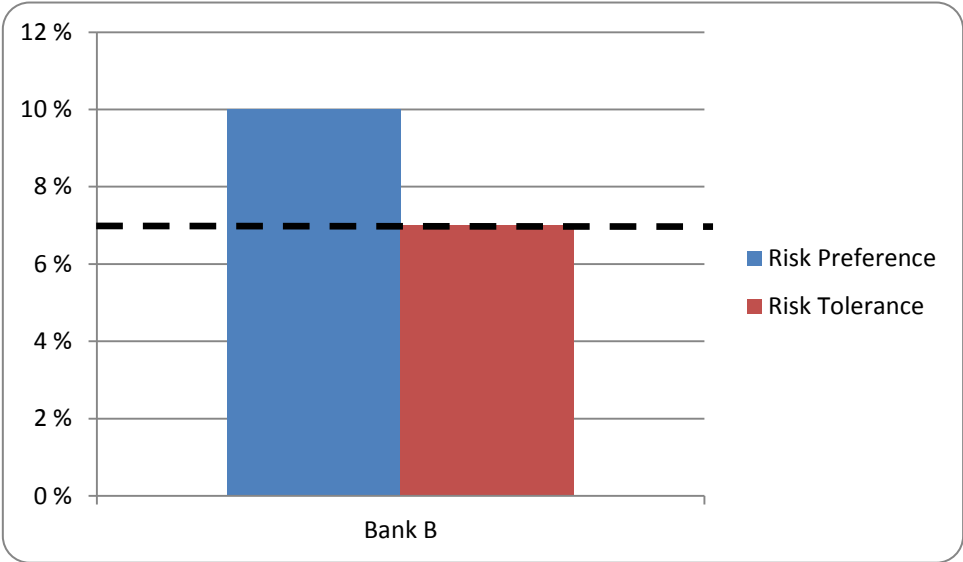


Figure 2.6 – High risk preference/Low risk tolerance

Bank B publicly states that the risk tolerance is currently lower than the risk preference which makes them unable to take on as much risk as they would prefer. Investors, as well as other stakeholders, will observe this and assume that this bank does not spend money on more risk-adjusting measures than necessary. Additionally they can also expect an increased operational risk profile if the risk tolerance should “loosen up”. This would attract short-term and risk-loving stakeholders to the organizations, which was the initial intention of Bank B.

2.4.4 Additional notes and opportunities

I have now demonstrated that RiskPAT will open up for stating and properly communicating risk profiles. Further on, it will also open up for other opportunities. One of these is *risk*

acceptance. Risk acceptance is, as previously mentioned, the A in RiskPAT, and could undoubtedly help strengthen the concept in practice.

Risk acceptance

In theory, the RiskPAT is a solid concept, but in practice it may be harder to execute. Operational risks change constantly and should be monitored at all times, but in real life there will always be a delay in this process. Consequently, the true risk profile will often lie a little bit outside of the RiskPAT's estimation. This is where the risk acceptance comes into play; the risk acceptance is a measure which states the *risk preferences allowed volatility*. This means that the board states a value which expresses what they see as an allowed buffer of the risk preference before any extreme measures are initiated. The risk acceptance will therefore benefit the RiskPAT by increasing the accuracy of its estimated true risk profile. It would also improve the measurement process and control of the risk profile, which will be further discussed in part three of the thesis.

Financial distress

I previously defined risk tolerance as a limit which, if bypassed, would cause *financial distress*. In most organizations this would be accurate, but the financial industry is put together a little differently. Investopedia, which is a credible business dictionary, defines financial distress as “*A condition where a company cannot meet or has difficulty paying off its financial obligations to its creditors. The chance of financial distress increases when a firm has high fixed costs, illiquid assets, or revenues that are sensitive to economic downturns.*” (Investopedia. 2012). It is rarely seen that a financial institution experiences what the definition explains. Financial institutions are monitored and regulated to an extent that the authorities would step in way before these events would occur. This means that the definition of financial distress in a financial institution's context should e.g. include “*or at a point where licenses and/or significant ratings are severely threatened.*” The essential point here is that risk tolerance should not state the point where a financial organization goes bankrupt, but instead state a point of where “things get out of hand” and the board loses control over the company. This might be hard to calculate, but it is also the most logical limit of the risk tolerance.

Terra Securities and Acta are good examples of banks that bypassed their risk tolerance. Terra Securities, a former Norwegian brokerage firm, initially entered financial distress after a scandal early in November 2007. This led to the authorities withdrawing Terra Securities' licenses which ultimately led to bankruptcy at the end of the same month (Dagens Næringsliv.

2007). Acta Kapitalforvaltning, which was earlier mentioned in Chapter 2.2, also passed its risk tolerance. They never suffered any problems with paying their creditors, but the authorities criticized them for un-ethical behavior and threatened to withdraw their licenses if they did not conduct a major transition, which they now currently are working on. Still, rating bureaus downgraded their recommendations of Acta, an act which was directly caused by their exceeded risk tolerance (Dagens Næringsliv. 2009-2012).

Both of these organizations bypassed their risk tolerance limit and ended up in financial distress, which led to bankruptcy in one case, and severe degradation in the other. This demonstrates that financial distress for financial institutions does not necessarily lead to bankruptcy, but that it represents a limit which seriously threatens the further existence of the company. No organization, financial or otherwise, would therefore willingly enter financial distress.

Business cultural influences

An additional note concerning business cultures should also be made. Business cultures have a huge influence on an organization's true risk preference. In order to make the RiskPAT as similar as possible to the true risk preference, the board will have to take extra precaution to the internal conditions when stating their perceived risk preference. This may cause the risk preference to be higher than the risk tolerance in a few cases, which is not a good state to be in. Acta Kapitalforvaltning, Terra Securities, Enron and Société Générale are all examples of financial organizations with a risk preference higher than the risk tolerance. It is not necessarily illegal to have a preference over the tolerance, but it will unquestionably lead to the organization's demise if it is not handled properly. This could be managed by either increasing the tolerance or by lowering the risk preference.

Increasing the risk tolerance will not necessarily involve adjustments to the internal culture, which in turn may lead to an increased risk preference over time. This is due to the tendency of the culture stretching past its limits, which implies that the pattern would repeat itself. To really take control over the organization again, one would have to take control over the culture by mitigating risks and assessing the dynamics of the incentive programs within the organization. This thesis does not aim to show how cultures can be changed, but to raise the reader's awareness of the influence that the business culture can have on RiskPAT.

Seasonality and cycles in operational risks

Whether seasonality should be taken account for in operational risk management is difficult to answer since it varies a lot. External fraud and IT-issues are mostly considered to be independent of changes in the economy and other seasonal changes. Other operational risks, such as natural disasters and rogue traders are, on the other hand, often associated with special seasons and/or states in the economy. If the operational risks that are dependent on seasonal changes vary sufficiently enough throughout a cycle, it would suggest that the risk profile would also be affected. This further, again, raises the question of including seasonality and cycles in the RiskPAT.

When handling seasonality in operational risks, one would have to choose between either adjusting the regulatory capital to hedge for the seasonality, or practice increasing/decreasing the risk exposure through every cycle. The first option would generally be preferable for risks that are too time-consuming and/or expensive to mitigate, while the other option would be preferred in cases where risk mitigation can be done on short notice and is relatively cheap. The biggest problem with seasonality, and the problem that this section focuses on, lies within the first group.

Let us assume the operational risk of a failing control process; the losses from failing control processes are reported to be higher during financial booms. This is due to the increased activity which overloads the control processes and causes an increased rate of failure. Control processes are often complicated and heavily dependent on advanced IT-systems. This would mean that the risk of failing control processes is time-consuming to mitigate and also highly correlated with business cycles. Consequently, it would be too difficult and costly to decrease/increase this risk during a financial boom/recession, which would further suggest that the best solution is to adjust the operational risk capital instead of increasing/decreasing the risk level.

In credit risk, there is currently a common practice to have a capital that is set aside to work as a buffer for seasonality. This capital can be decided by either using a method called *point-in-time* (PIT) or a method called *through-the-cycle* (TTC). All of the following information has been collected from Sparebank 1 SR-Bank's risk report from 2011 (Sparebank 1 SR-Bank, 2012). PIT is a method that adjusts the capital at any time throughout the cycle to reflect the current fluctuations. This method is more appropriate for short-term changes due to the constant fluctuations in the risk capital, which would be quite expensive. When it comes to

calculating risk capital in the long-term it will, however, be more optimal to choose the TTC approach which calculates the capital with regard to the long term trend for the risks loss. TTC is a method which overestimates the need for capital in “good” times, and underestimates it in “bad” times. This is somewhat similar to Keynes’s macro-economic theory on saving money in good times and spending them in bad times. By using TTC, it would create an effect that dampens the fluctuations of the seasonality, but since the approach does not take the exact fluctuation at the time into the calculation it works poorly for doing a “status check” or through extraordinary cycles. Figure 2.7 is a graph that illustrates, both, the PIT- and TTC-method explaining the needed capital for the operational risk from the example in the last paragraph.

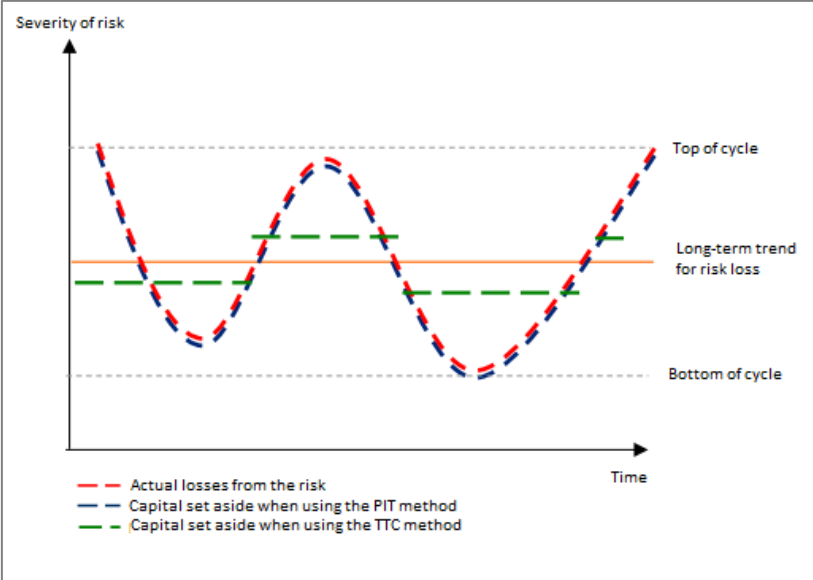


Figure 2.7 – An edited illustration of the PIT- and TTC-method (Sparebank 1 SR-Bank. 2012).

We can see that during financial booms there is an increase to the losses from the risk, while in recessions the severity is significantly decreased. Sparebank 1 SR-Bank has chosen, in credit risk, to combine the methods to both reflect the current point of the cycle while still dampening the fluctuations, but could the same combination of methods be used to stabilize the fluctuations of operational risks as well?

Handling seasonal fluctuations is necessary to stabilize the risk profile so it can be known at any time. The problem with doing it with operational risks is that all of the risks are so widespread that almost each of them follows a different pattern. To get an overview it would therefore be advisable to sort the risks by which seasonal pattern they follow. Some, like the previously mentioned risk, may follow business cycles while other risks (e.g. natural

disasters) may follow an annual cycle. These risks may be pro-cyclical or counter-cyclical and some operational risks may not even follow a pattern at all. If all of the risks were sorted, it would be easier to see how much the seasonality really affects the true risk profile.

Seasonality is clearly a variable that could have an effect on the accuracy of an organization's RiskPAT. However, I will not discuss this variable further in the thesis except for mentioning it briefly in Part three.

2.4.5 Pitfalls, and ways to avoid them

There are certain things to avoid if the implementation of RiskPAT should be successful. First of all, **one should only use one definition for each of the terms**. Since the current state of “risk appetite” is over-encumbered with definitions and different perceptions, which has made it useless, one should not waste this chance by defining risk preference more complex than it really is. The same goes for risk tolerance. Choose the definition that explains bullet point (2) in Chapter 2.4.1 best, and stick with it. By using relatively brief and concise definitions, and possibly combine them with a case or an example, one can avoid much confusion.

Secondly, **do not be afraid to over-expose the definition in the initial phase of the implementation**. The previous survey, and the discussion of current definitions, show that there is confusion around some risk-terms; particularly the term risk tolerance. One should just assume that this is the case within your bank as well, and therefore be prepared that the people within the organization will initially perceive the terms differently. A simple definition should be attached where ever the term is used until it is assumed that all who are exposed to it will understand it in the same way as everybody else.

Finally, one should **be honest**. In the end you do not fool anyone other than yourself if you state an untrue risk preference. The whole concept is not only meant to increase the boards control of the risk, but also as an easier way to communicate the risk profile to external stakeholders. Cheating with RiskPAT numbers could easily be revealed through risk losses in the financial statements, which is why RiskPAT is such a reliable tool for investors to avoid investing in banks with risk preferences that are higher than their tolerances. The true risk profile (the lowest of the preference and the tolerance) is the value that really counts towards indicating the present risk management, while the relationship between risk tolerance and risk preference is more of an indication of what to expect in the future.

2.4.6 Summarizing RiskPAT

The concept which I have presented and discussed in this chapter, will help any organization to get rid of the confusion around an organization's risk profile. By being concise to use the risk preference with an accepted variability zone (risk accept) and the risk tolerance, all concerned parties will soon enough learn to know what each of them indicates and stands for. Once a common understanding of these terms is achieved, it will be a tremendously beneficial tool for the board to both communicating and controlling the organization's risk profile. An illustration of RiskPAT can be seen in Figure 2.8.

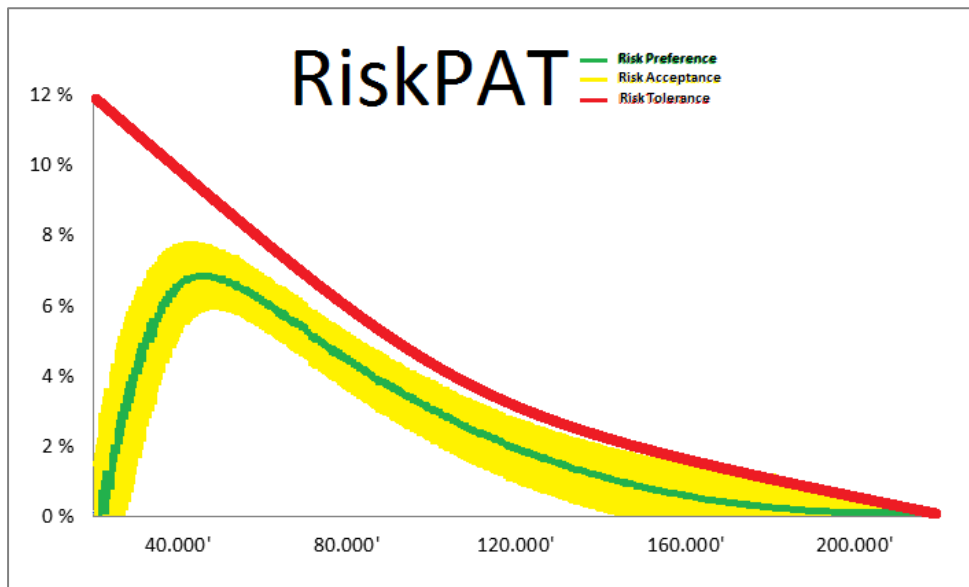


Figure 2.8 – An illustration of RiskPAT

2.5 Conclusion

The time where risk appetite still had an opportunity to be reviewed and re-designed has long passed. It took too much time before anything was done to ensure a common understanding of the term. This made the term evolve into several directions. In this chapter, I have therefore concluded that risk appetite should be discarded in favor of RiskPAT. RiskPAT uses a variety of three terms to improve both communication and control over an organization's risk profile. Risk preference is a new and easily adaptive term, which is un-burdened with varying perceptions and definitions, while risk tolerance is already a well-established term in the market. Although the survey from Part one revealed some ambiguity in the perceptions of risk tolerance, I have still chosen to continue the use of it. Risk tolerance is the most natural term to use in RiskPAT and I believe the existing ambiguity easily can be defeated if the users are consistent with it when using it. Risk acceptance is the third term which RiskPAT uses. It has a relatively minor influence on the concept, but could still prove very useful in a practical setting. By creating a zone around the risk preference, risk acceptance allows for small natural fluctuations to occur without causing too much reaction. This makes the RiskPAT adapt something from the ALARP-principles by creating a zone which is not intolerable, but not necessarily negligible as well. This will be discussed further in the next part.

By using RiskPAT with a properly measured risk preference and risk tolerance, every financial institution and its stakeholders could get a much better grip on the organizations true operational risk profile. This would be beneficial to all parties, but some institutions might have higher incentives to implement this than others. The next part will discuss incentives that are in the market for implementing RiskPAT as well as discussing some operational measurement-techniques which would further improve communication of the risk profile on an internal level.

Part III
- Optimizing the Benefits of RiskPAT -

3.1 Introduction

This part will mostly address the problem of successfully communicating the risk profile internally within the organization. First, however, I believe it is important to properly discuss which incentives that currently exists, or rather lacks, for the financial institutions to implement RiskPAT. This will be discussed in Chapter 3.2.

For RiskPAT to become a success, it is not enough to manage the external communication. Internal processes would have to be optimized for the allowance of proper and flawless communication of the risk profile. When implementing RiskPAT, one would have to set an overall risk preference and coherent risk acceptance, which would have to be broken down into objectives for each department of the organization. These objectives would then have to be measured and communicated upwards again to the board. This involves a lot of communication which could easily lead to misunderstandings if the proper tools are not applied. Chapter 3.3 will discuss the optimization of measuring techniques and the metrics that these techniques use, with the intention to improve how operational risks are expressed internally.

Chapter 3.4 will conclude the discussion on the necessary conditions and internal processes that needs to be present for optimizing the benefits of RiskPAT. It will further work as an introduction to the final part which will conclude this whole thesis by reviewing RiskPAT and suggesting future possible research within the field.

3.2 Incentives for Implementing RiskPAT

Any new concept that is introduced may just seem like expensive changes to some managers. Consequently, there always have to be an incentive which makes the concept's benefit exceed its cost. RiskPAT would definitely bring the organization's operational risk management to a new level, but this may not always be sufficient enough. Some managers might want proof of the benefit in monetary terms, in order to approve the implementation. This may be benefits such as reduced risk capital, reduction in un-/expected losses or simply increased revenues. The hard truth is that most board-members and managers will not open the organization's pockets until it is either demanded by the authorities or it promises value in monetary terms. Currently, there are only a few regulations which incentivize the implementation of concepts such as RiskPAT. This chapter will take a closer look at these regulations and their combination with risk-environments that allows for the maximization of RiskPAT's benefits. It is, however, important to see that even without incentives, RiskPAT would still in any case yield benefits to operational risk management, which will be proved with the following comprehensive example from the recent financial crisis.

3.2.1 The financial crisis

Lasse Andersen presented a review of the financial crisis from an operational risk-context during a lecture at UiS, which included material I will use in this example (Lasse B. Andersen. 2011). In the wake of the financial crisis a structured and complicated product known as a Collateralized Debt Obligation (CDO) was developed. This product consisted of many individual mortgage obligations which was pooled by mortgage brokers, rated and sold to investment banks which in turn had these CDO's insured. It would be too extensive to go into close details on the subprime-crisis, and several previous master theses have already been written on this subject. The reason why I mention this crisis is because I believe a great deal of it could have been avoided if the communication and awareness around the included parties' true risk profile had been better. The CDO were typically marketed as a very low-risk product, which made most of the market risk "disappear". The actual case was that the complex structure of the product transferred more and more risk into operational risk. Every involved party probably knew that things were handled in an un-ethical way, but they were still making money so they kept going.

Mortgage brokers

The mortgage brokers guaranteed loans without credit checks since they had close to zero business risk. As soon as a mortgage was given, they bundled it together with other mortgages

into CDO's and sold them to investment banks. A mortgage broker called Quick Loan Funding Inc. even marketed their mortgages with the slogan: "No income verification. Instant qualification." These aggressive sales techniques combined with poor credit evaluations of the customers all comes from bad operational risk management, which ended up with transferring a lot of market risk to the owners of the CDO.

Rating Bureaus

The companies that were responsible for credit rating these CDO's had massive workloads during this period. Figure 3.1 shows the increase in work that these bureaus experienced while lacking increase in staff.

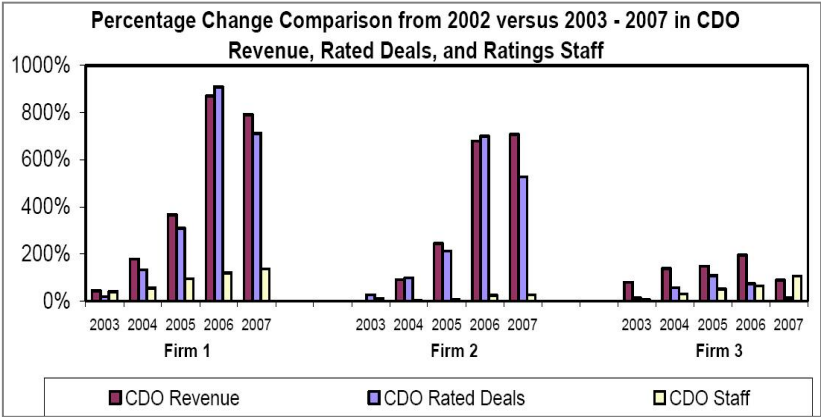


Figure 3.1 – Activity in rating bureaus from 2003-2007 (Lasse B. Andersen. 2011).

Firm 1 is the most extreme, which had an increase in CDO ratings by nearly 950% in 2006 compared to 2002 numbers, while the number of staff working with these deals had only been doubled in the same period. This posed a massive operational risk since the time spent rating each deal was dramatically reduced, which resulted in a decrease of competence among the workers and most of the deals to be AAA rated (even though this was far from the true rating. See Figure 3.2).

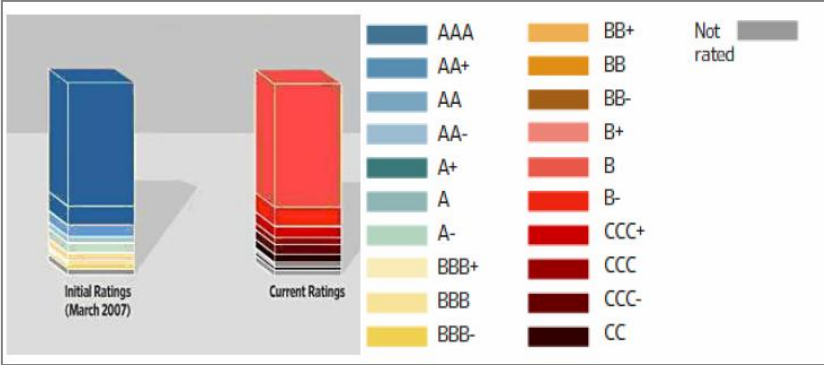


Figure 3.2 – CDO ratings' change over previous years (Lasse B. Andersen. 2011).

Further, this transferred a substantial amount of market risk to CDO owners which now thought they owned a grade AAA CDO, and also a lot of risk to the insurance companies which thought that these CDO's could safely be insured with little or no losses.

Insurance companies

The insurance companies worked as a buffer for the investment banks (the owners of the CDO's) when everything started to go wrong. The investment banks that owned a CDO bought a credit default swap (CDS) from the insurance companies for a series of payments. In return, the CDS promised that if the CDO should default at any time, the insurance company would buy back the bond for its par value. The insurance company had aggressive incentive programs which granted very good employee bonuses for sales of CDSs. The insurance companies could not foresee that the AAA ratings were not correct, but focus on profits and the bonus solutions were operational risks that probably made the brokers oversee certain warning signs (Lasse B. Andersen. 2011).

Investment banks

The investment banks were arrogant about risk throughout this period. Lasse Andersen states in his lecture "*Sept. 2007 Citigroup owned \$43 billion in mortgage related assets. Mortgage default probability considered too small to be included in risk analysis.*" (Lasse B. Andersen. 2011). When Citigroup discard the element of mortgage default in their risk analysis, it clearly shows signs of bad risk management. The incentive and bonus programs were not justifiable either, which meant that the investment banks kept on buying CDO's and blindly relying on the rating bureaus and the "safety" granted from the insurance companies. This culminated in bankruptcy for several of the investment banks, which furthermore meant that all the losses incurred on the shareholders and other stakeholders of the companies.

I believe that all of these mentioned mistakes throughout the companies could have been prevented or at least been reduced if the companies had used a more thorough operational risk management. Let us now take a look at the operational sources behind the crisis with the RiskPAT in mind. It is most likely that a lot of this could have been prevented with a properly set risk profile and proper communication of it, both within and outside the companies. If the rating bureaus had implemented RiskPAT they would probably have had a risk preference which would most likely have sent out an alarm signal when the ratio between *CDOs to be rated* and *number of workers* drastically increase. Since the risk preference is the level where the board wants the risk profile to be at, it would consequently contribute to direct mitigation of this risk, which would further have led to the CDO's being more accurately rated. The

same would have gone for all of the other institutions that suffered from operational risks as well. The Basel II framework, the most central tool towards improving operational risk management, had already been established by this time, so why did these errors still occur?

Firstly, external risk communication, which was covered in the last part, is extremely different from the internal communication. When communicating externally you can simply state the values from the RiskPAT and let the analysts and investors do the rest of the calculations. When communicating internally, however, the RiskPAT needs to be broken down into criteria which covers each operational risk and then properly communicated back to the board/risk committee which supervises and controls the risk profile internally. This process has to be done without misunderstandings, since ambiguity could ruin the whole concept. This will be covered in the next chapter, where the thesis discusses metrics and measurement techniques that give easy and communication-abled results.

The second reason behind the increased operational risk profiles throughout the financial crisis could, as earlier mentioned, be caused by negative incentives to improve risk mitigation. Some of the operational risk approaches in the Basel II framework incentivize capital in front of risk mitigation. Having a high regulatory capital that is based on income, an attribute which is mostly unrelated to the true operational risk level, did not help throughout the subprime crisis, but the RiskPAT concept might had.

The Basel II framework certainly offers an improvement to operational risk management, but obviously not to an extent that the institutions has an incentive to implement risk reducing measures such as RiskPAT. In the next sub-chapters I will explore the Basel II framework further, and explain why not all the approaches that it includes give incentives for risk mitigation.

3.2.2 The Basel II framework: Basic indicator approach and Standardized approach

As concluded in part one, the BIA and the SA are both methods that focuses more on setting a regulatory capital aside rather than on incentivizing preventive measures. In addition, both of the methods have poorly chosen KRI to calculate the regulatory capital. Let us take a look on the benefits that Bank C would receive by implementing the RiskPAT while using either of these approaches:

The board of Bank C knows that bad operational risk management often leads to bankruptcy which has made them decide to take proactive measures by implementing RiskPAT. The board sets a risk preference, which is successfully broken down and communicated to all sub-

divisions. They find that the brokers in the markets department have incentives that are so profit-focused that a lot of the employees have started acting recklessly and un-ethical. To reduce this risk, the manager of this department redefines the bonus terms and arranges social gatherings to increase solidarity to the workplace, which turns out to work perfectly. The department does not experience any changes to their income level since the workers are still incentivized, but in a better and healthier way. Bank C now has a substantially decreased probability of incurring operational risk losses, but the regulatory capital only decreases with a fraction (the cost of implementing the measures). I would not say that the experienced incremental decrease in income is at all correlated with the amount of risk that was mitigated. Currently, it is not until an organization starts using the AMA that the implementation of RiskPAT might be more beneficial, but it should not be this way. Ideally, authorities should find another KRI for the BIA and the SA that will help the capital to better reflect the organization's true risk profile, which would further incentivize the management of the risk profile.

3.2.3 The Basel II framework: Advanced measurement approach

The AMA is the only approach in the Basel framework that incentivizes an implementation of RiskPAT, but not any form of AMA. As mentioned in part one, an organization should create its own loss distribution which can include any mix of expert opinions and objective data, but for the RiskPAT to be beneficial, the risk distribution needs to properly reflect the organizations true risk profile.

Figure 3.3 illustrates a common loss distribution that operational risks tend to have.

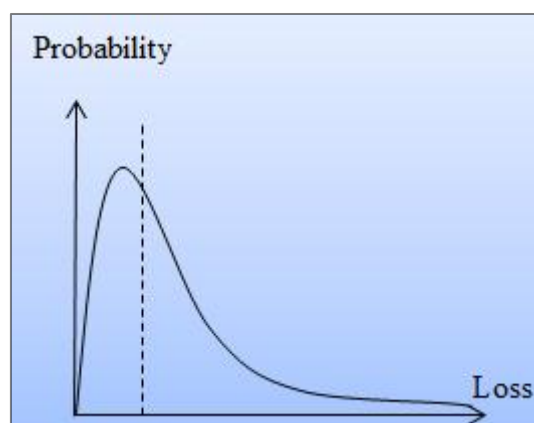


Figure 3.3 – Common operational loss distribution (Häger, 2011)

The dotted line illustrates the difference between the expected loss (EL), which is on the left side of the line, and the unexpected loss (UL), which is found on the right side. The guidelines to making the operational risk distribution are, to a rather large degree, made open for interpretation: *“667. Given the continuing evolution of analytical approaches for operational risk, the Committee is not specifying the approach or distributional assumptions used to generate the operational risk measure for regulatory capital purposes. However, a bank must be able to demonstrate that its approach captures potentially severe ‘tail’ loss events. Whatever approach is used, a bank must demonstrate that its operational risk measure meets a soundness standard comparable to that of the internal ratings-based approach for credit risk, (i.e. comparable to a one year holding period and a 99.9th percentile confidence interval).”* (Basel Committee on Banking Supervision, 2005). This wide statement has led to organizations using their acquired skills within market- and credit risk for calculating the operational loss distribution. The processes used in market- and credit risk to create distributions often needs huge amounts of data to be statistically significant. This generates a problem since operational risks does not tend to the required bases of historical data. Any bank will probably have a rich database of the regular losses (high probability and low severity) which contains enough information to predict the EL, but the problems occur when UL needs to be estimated. The data that is needed to estimate UL is rare, because they happen rarely and banks with these kinds of losses often goes bankrupt. Even if a bank manages to withstand a severe loss, it would probably cause huge adjustments to the banks infrastructure, which again would make the collected data invalid. This has to a certain degree been solved by cooperative databases, which are based on banks sharing data with each other to create one huge database with operational loss information that could make a whole distribution statistically significant.

Further on, this would work against its cause, since data that is collected by other banks about operational risk is mostly irrelevant, which again would cause the distribution to be irrelevant. Operational risks are specific for each bank and every time an enormous operational risk occurs it will either cause bankruptcy or major changes, which again would make the historical data invalid. The fact is that there, most probably, never will be a statistically valid distribution of a bank’s operational losses as long as the focus is on using mostly objective and backwards-looking data. This means that another approach has to be made for the risk distribution to properly reflect the organizations true risk profile.

To create an incentive to use RiskPAT and other proactive risk tools, one needs to have data from expert opinions represented in the loss distribution, since it is only then that risk mitigation will grant immediately visible benefits. When risk mitigation is done, the experts can foresee that the risk is reduced and include it in the distribution, which in turn will decrease the regulatory capital. Now the operational risk management is forward-looking thanks to expert opinions, and also has the possibility to free more capital by mitigating more risks.

3.2.4 Current incentives for mitigating risk through the new concept

Today, AMA, with enough data from expert opinions, is currently the only approach that makes the regulatory capital reflect the true risk profile, and furthermore fully incentivizes the use of RiskPAT. This narrows the present field of interest a lot, but the authorities should not let it be like this. The government and other regulatory authorities could benefit by reviewing the approaches and creating incentives and/or regulatory needs to implement proactive methods which mitigates risks instead of just focusing on the consequences of it. The regulatory should at least be based on a KRI that would more properly reflect the organization's true risk profile, which is the most important attribute for incentivizing RiskPAT. This chapter has discussed who might have incentives to actively use RiskPAT. The next chapter will go on to discuss the problems of internally managing and communicating risk profiles.

3.3 Internal Communication and Control of the Risk Profile

The main focus of this chapter is to discuss the current problems the banks are facing today when internally communicating their risk profile. As mentioned in part one, it is currently most common to use risk maps to communicate individual risks. It is, however, not only the technique that is essential for improving the communication, but also the metrics that are used. This chapter will start off by presenting a discussion on selecting the proper metric.

3.3.1 Selecting the best metric for communication

The survey I conducted shows that many financial organizations are currently using points to measure both the severity and probability of its operational risks. In fact, 75% of the respondents that measures their risks individually in a quantitative manner, have chosen to use points as a metric instead of amounts. Using points for measurement is easy and time-saving for any sub-unit managers that report the risks, but it may also be a source for miscommunication like in the following example:

Bank D has planned to focus on stating a risk preference and use it actively to increase the control over the organization's risk profile. In order to get an impression of the bank's current situation, the board gets a risk committee to send out a risk map to all the sub-divisions which in turn fills the risk map out and returns it to the risk committee. Both, the severity and the probability are reported as points on scale from 1-10. The risk committee then combines all of the returned risk maps and includes in their assessment which they present to the board. When the risk committee presents their assessment, the board gets overwhelmed with points which they really have no relation too. The only thing they feel they can do is to combine all of these points into a distribution and see at what level a reasonable risk preference can be set.

This is a perfect example of how not to use points if there even is a proper way to use points in risk measurement. The main problem with using points is that they have no value when related to each other. If a person had all the information of the sub-divisions, and that person filled in all of the risks into a risk map, this could have been avoided, but this is never the case. In fact, the most basic mistake that can be done is to directly compare different risk maps with each other. The manager of an operational department might rate a loss of \$1000 as a 10 in severity, while the same amount would probably only score a 2 if it was rated by a manager in the markets division. This would result in the board using massive resources to mitigate the risk that scored 10 in the operational department, which in reality would only contribute with marginal savings compared to the mitigation of another potential risk that

scored 5 in the market division. As we see from this, it is simply impossible for any board to prioritize and compare risks with each other if they have no real value to relate to.

To solve the problem of prioritizing correctly when comparing points with each other, there exists something called conversion tables, which helps to make all the points relatable. A typical conversion table can be seen in Figure 3.4.

| Department | Markets | Operations |
|-----------------------------------|---------|------------|
| Department Severity (points 1-10) | 3 | 10 |
| Multiplier | 2 | 0,3 |
| Organization Severity (points) | 6 | 3 |

Figure 3.4 – A simple conversion table

The department severity is the points that the manager sets to illustrate a certain risk in his department, while the multiplier is a set level which reflects the departments value at risk (VaR) compared to the organization’s VaR. The department’s points are then multiplied with the multiplier which equals the organization severity, which is given in points that are comparable with each other. In this figure, we can now see that the board would preferably mitigate the risk in the market department before doing anything with the risk in the operations department.

There is, however, a problem with these conversion tables as well. Of course it improves the system of using points, but after you have found the multiplier for each risk by researching the VaR in each department, you have basically done approximately the same amount of work that would initially be needed to use amounts instead of points. Amounts as a metric will always be much more relatable and more beneficial. An organization would never have a risk preference that stated: “We shall not exceed a risk level of 49 points”, because it would be confusing and un-relatable by anyone that read it. The metric used to measure risk should be easily communicated and directly relatable to the set risk preference of the organization, and the best way to do this is to use amounts. It may be more demanding to implement, but it is a sovereign metric compared to using points. Now that the discussion around metrics is concluded, I will continue to discuss the different measurement techniques which optimizes internal control and communication.

3.3.2 Risk maps in the financial industry

Part one stated that risk maps are most likely derived from the petroleum industry and its similar ALARP-principle. Even though risk maps have some important principles, they are not, in their current form, optimized for communicating risk profiles. It is currently too hard to place risks for the managers and the dynamics of the technique seems much more suited for operational risk management in the petroleum industry than in the financial industry; in the petroleum industry there is more of a binomial property to the outcome of risky events, which makes placement of risks easier. In the financial industry the outcomes are not so binomial.

Let me illustrate with an example:

On an oil rig, there is a probability of 0,0001% (during one year) that a fire will start in the control room and the sprinklers in the same room will fail to deploy. If a fire would occur in the control room, and it failed to be extinguished, it would be likely that 50% of the people in the room would suffer fatal injuries. If there is regularly two controllers working each shift, and the statistical value of a life is set to \$7 million, one would have an expected loss of \$700 on a yearly basis. In this case it is very easy to place the risk on a risk map, and the placement will be communicated to anyone who reads it without any chance of miscommunication. Now let us look at a typical operational risk in the financial industry: In a bank there is a probability of 0,01% (during a year) that a transaction with a typing error is created and the computer system fails to control it. The losses that this event would incur on the bank can be everything between \$10 and \$10 million, which makes the yearly estimated expected cost to be anything in the interval \$0,10-\$100.000. According to the current practice, an average of the loss interval would be made to place the risk at an estimated \$50.005, but is this the best way to do it?

Figure 3.5 illustrates the placement of the risk from the last paragraph in a risk map.

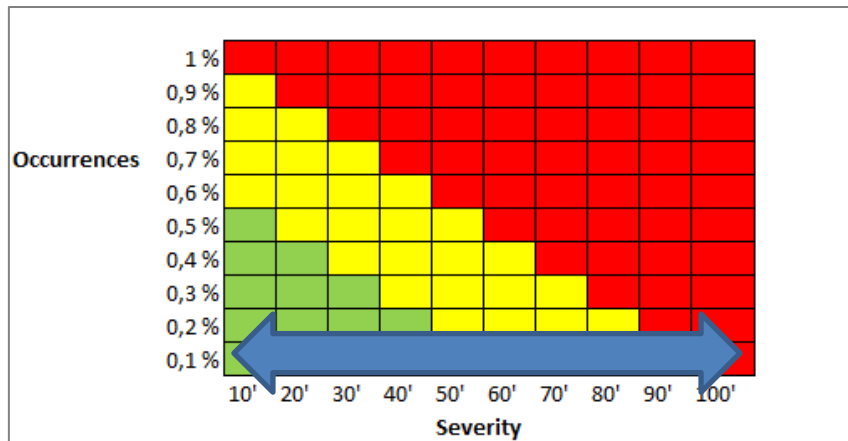


Figure 3.5 – Placement of operational risks in a risk map

The risk has a very low chance of occurring so it would be at the very bottom of the Y-axis, but what about the X-axis? Some of the managers would probably say that it would most likely only end up with \$10 losses which would make further attention unnecessary, while another could claim that the losses probably would be at \$100.000. Technically, the loss could be placed anywhere along the blue arrow, but the current practice would calculate an estimated loss of \$50.005 and place it there. Would not such an approach erase a lot of important information of the risk that should actually be reflected in the risk profile?

Think of a case where one manager believes there is a 0,01% chance of incurring losses of \$100.000, while another manager thinks that the same event had a 1% chance of incurring a loss of \$10. If this is treated without looking into the specific managers opinions, one might just take the average of the probability and match it with the average of the severity. This would make it ranked at (5,5) in Figure 3.5, while both managers actually thinks that the estimated expected cost is respectively \$10 and \$0,10. Perhaps it may be hard to think that these examples may occur in the real world, but they do.

Another feature of the risk map that is being criticized is the fact that it will never be used to its full extent. Not a single financial organization would naturally have a risk that scores a high probability as well as a high severity. Consequently, the upper right part of the map is completely useless. This is only a small esthetical problem, but it helps pointing out that risk maps may not be the best tool for measuring operational risk in the financial industry, which brings us over to the next sub-chapter.

3.3.3 Risk distributions

One way to avoid the known problems of risk maps, and still include the most important principles of it, would be to create loss distributions of all possible risk events. This will certainly be more work-demanding initially, but the results will undoubtedly grant huge benefits towards an organization's communication of their risk profile; In addition to allowing more precise and accurate communication of the risk it also makes it easier to control each risk up against the objective that is decided by the risk preference and its coherent risk accept zone. If a distribution is set up for each operational risk it will include a standard deviation which can illustrate a risk's heavy tail much better than any risk map can.

Let us again take the last example from Chapter 3.3.2 where there were two managers who disagreed on the divisions risk exposure: One of the managers thought there was a high occurrence of errors with a low severity, while the other was convinced there was a low occurrence of errors, but that the errors tended to be of a severe degree. The theory behind the risk map would handle this by averaging both the probability and the estimated loss, and place it in the middle (Figure 3.6).

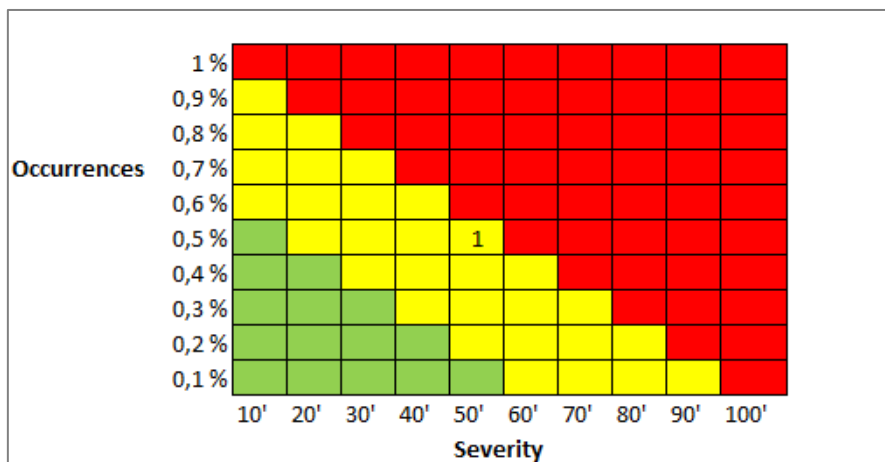


Figure 3.6 – Risk map representing risk from Chapter 3.3.2

The risk would now quite possibly be monitored and maybe also mitigated, but it would be difficult to decide which actions that should be monitored or even where to start mitigating. Let us look more closely at the example. The reason why the first manager thought that the typing error would happen often with non-severe losses is because of the employees working long hours, and that there are observed a lot of minor errors during late hours. The most severe of these mistakes are caught by the controlling processes, but many minor mistakes avoid these controls which incurs a number of small losses. The other manager did not think of the first risk, but instead of a risk concerning their top salesman. Their top salesman which

has a key role in sales department and is considered invaluable has recently shown tendencies to immorality. This salesman knows how all the control-processes work and could easily manufacture a typing error for own profits. This is, however, a scenario that is considered to be very unlikely to occur. Both of these are actions that could lead to an operational loss caused by typing errors, but by averaging the losses and the probability both of them completely loses their distinction. This makes it impossible to know where to start mitigating, and could further lead to unnecessary actions, such as implementing measures to decrease the *amount* that is lost during minor typing errors instead of decreasing the *probability* of it, which would grant significantly higher benefits.

Now, if the same risk had been approached with the intention of creating a loss distribution, both of these individual examples would have been reflected in the distribution in Figure 3.7.

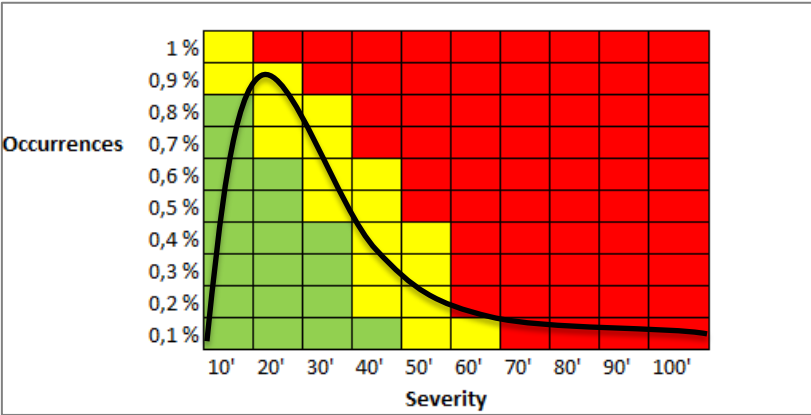


Figure 3.7 – Risk map with a distribution of the risk from Chapter 3.3.2

We can now see in the figure that the position where risk 1 was placed in Figure 3.6 is not even close to the true distribution. We can also see that the risk map’s red and yellow zones have shifted inwards to illustrate that the true dangers of operational risks is their heavy tails. Although this approach looks a little different from a regular risk map, it still contains the same theories and principles. The part of the risk that is considered yellow should still be monitored while the red parts should always be mitigated if possible. If the organization had used this approach instead of risk maps in the last example, both of the managers opinions would have been properly reflected, which would have made the job with asserting the risk at a later stage much easier. The distribution simply breaks down the problems to show two different peaks to work with instead of one. This means that, when applying the RiskPAT, a risk preference could be set for both the occurrence and the severity of each risk. This could be supplied by a coherent risk acceptance, represented by the yellow zone, which again allows

for natural fluctuations. By dividing these two issues for individual mitigation, instead of mitigating a product of them, one will cause the operational risk profile to be much easier to communicate and more in line with the true risk profile. This is something that definitely works as a major advantage to the RiskPAT.

Again, this discussion leaves us at where the discussion around the AMA in the last chapter ended. We know that subjective information is needed since relevant objective data is mostly non-existent when it comes to uncommon operational risk losses, but where can we find relevant subjective data? The answer was partly revealed earlier in this chapter; the manager that had concerns about the top salesman is an expert on his division. This risk could probably not have been discovered by any other sources than this manager, and the manager could probably also supply with information about the probability and severity of this risk as well. It is paramount that expert opinions like this are used for what it is worth. Many would probably agree with this, but would further state that it would be hard, or even impossible, to convert these expert opinions into numbers which can accurately make a distribution. This is not entirely correct. There is a tool which can help with this, and it is known as Bayesian networks.

3.3.5 Bayesian networks

Bayesian networking is briefly explained as a graphical probabilistic network which makes it easier to quantify expert opinions and merging them with historical data. The whole concept behind Bayesian networks is based on cause-and-effect by breaking bigger problems into smaller ones to see the “bigger picture” (Figure 3.8).

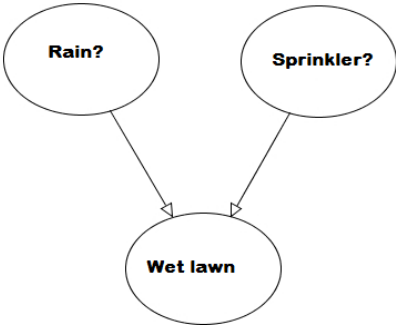


Figure 3.8 - Bayesian network (Häger, 2011)

The Bayesian network step away from the classic approach to probability, and uses the Bayesian approach instead which is much more fitting for operational risks, where a sufficient

amount of relevant data to create a statistically significant distribution may never exist. While the classic approach assumes there exists an objective truth that can be discovered through an infinite amount of data (law of large numbers), the Bayesian approach assumes there are no such true values and that the only thing we can do is to express our beliefs through probabilities. The uncertainty of the classic approach is expressed as the difference between the estimate and the outcome of the future event. The Bayesian approach on the other hand, explains any outcome of future events as an uncertainty, but that the degree of the uncertainty should be interpreted with respect to our expressed belief (Lasse B. Andersen. 2011).

Let us use the example from the last sub-chapter to create a Bayesian Network which calculates the probability of a typing error, using objective data and expert opinion (Figure 3.9).

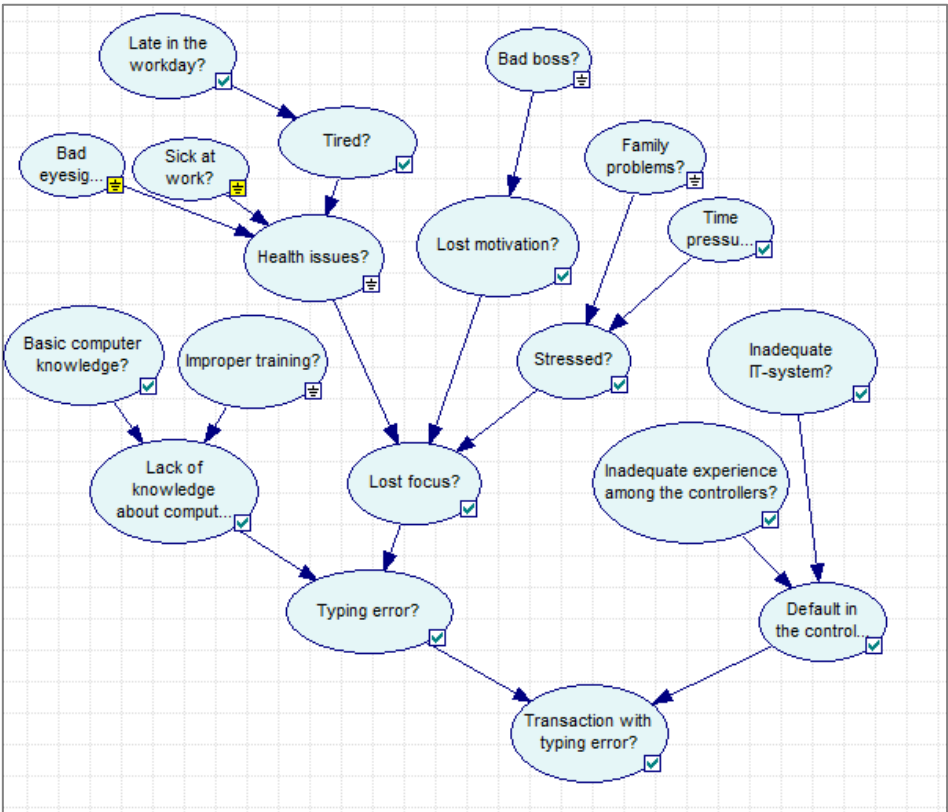


Figure 3.9 – Bayesian network of a typing error

The figure shows a detailed Bayesian network, which can contribute to create a loss distribution of the risk and also make it much easier to mitigate risk in the long run. All of these nodes could have been decided by the managers of the sales department to have an effect on the probability of a transaction with typing errors occurring. Each of these nodes are then connected to each other in a cause-effect pattern, which is completed with the final node

which shall state the probability of a transaction with typing error to occur. After this mapping is completed, one needs to assess all of the nodes and assign Bayesian probabilities to all of them. Probabilities like “Sick at work?” and “Bad eyesight?” can probably be found in objective data at the HR-department, while probabilities like “Improper training?” and “Inadequate IT-systems?” can be gathered within the organization from the respective experts’ opinions. I could get more technical in explaining the statistics in detail, but it would be counter-effective in this thesis. If you should want to read up on the use of Bayesian networks in operational risk management I can refer you to a former assignment on the subject I have written, which can be sent on demand.

After all the probabilities are assigned and used for a risk distribution, it is also much easier to handle risk mitigation. Due to the cause-effect dynamics of the network, it is also more intuitive, for all concerned parties, to see which nodes that currently are the most sensitive to changes by doing a sensitivity analysis which is illustrated in Figure 3.10. The bolder an arrow is, the more sensitive the connected node is to change.

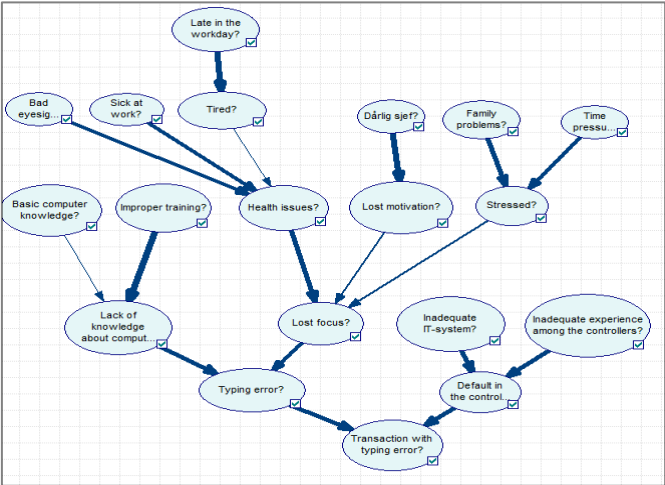


Figure 3.10 – Sensitivity analysis

Another advantage with Bayesian networks that makes it more fruitful to use is further experimenting with this sensitivity. Figure 3.11 is the same as the network in Figure 3.9, but is now in bar-format and displays every nodes Bayesian probability.

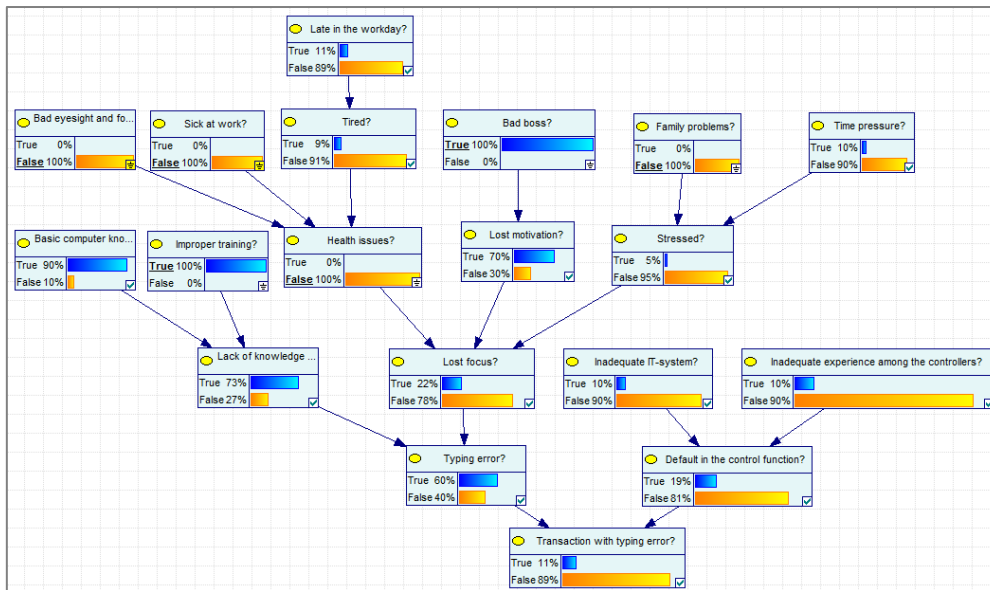


Figure 3.11 – Bayesian network of a typing error in bar format

The nodes where “True” or “False” is underlined, is where the user has determined the variables to see the consequence. From the figure we can see what the chance of a transaction with a typing error is when conditions like e.g. a bad boss and improper training is true. Bayesian networks can further be extended to include amounts as well as probabilities to proper calculate distributions. This is a relatively new approach, but also a very good way to implement expert opinions on the banks BEICF and information from scenario analyses into a loss distribution.

It was mentioned in part two that RiskPAT could offer the opportunity to implement seasonality and trends, and Bayesian networks may be a way of practically doing this. By using Bayesian networks, you can adjust for cycles if you assess the distribution on a regular basis. Let us take a look at a basic example where a Bayesian network is made around the chance of the IT-server in the organization to fail. The server-room is dependent on a cooling system to function, which in turn has proven to have problems with running during the winter. The simple Bayesian network in Figure 3.12 illustrates this.

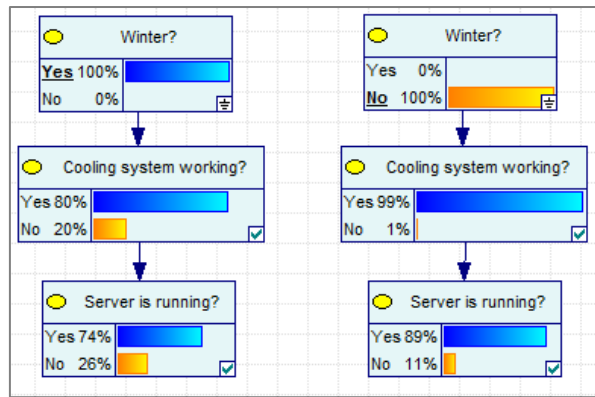


Figure 3.12 – Seasonal aspect with Bayesian networks

The probability that the server is running changes when the season is determined. This does not only have to concern annual seasons, but could also be a way to reflect economic cycles such as recessions and economic booms. This approach could therefore make the withheld capital and RiskPAT a much better reflection of the true risk profile throughout cycles as mentioned in Chapter 2.3.4.

3.4 Conclusion

Certain conditions need to be present in order to encourage and optimize the implementation of RiskPAT. Currently, the only approach in the Basel II framework that seems to incentivize RiskPAT, as well as all other proactive measures, is the AMA, with sufficient use of expert opinions. This is the only approach where the regulatory capital is calculated on relevant and forward-looking data, which reflects the organizations risk profile at any time. The fact that the organization's risk profile is only reflected in the regulatory capital in one specified approach, out the three, is actually shocking; any financial organization that is not using this specified approach is currently dis-incentivized to perform risk mitigation, and operates with massive, and partly esthetical, regulatory capitals instead. To avoid another financial crisis based on confusion around operational risk, I believe risk mitigation should immediately be incentivized by the authorities.

This part has also reviewed the internal processes which would be essential for an accurate RiskPAT. There are immense amounts of data that has to be communicated, both, upwards and downwards within the organization when implementing the risk preference, and its coherent risk acceptance zone. This communication is prone to misunderstandings and ambiguity in every joint of the process, which could bias the link between the organization's true risk profile and the risk profile that RiskPAT estimates severely. I wholeheartedly believe that any operational risk should be quantified in monetary terms and expressed through distributions that are created by Bayesian networks. This will be further reviewed in the next, final part, which will summarize the whole thesis and suggest future research which could further improve this field.

Part IV
- Reviewing RiskPAT and the way forward -

4.1 Reviewing the Thesis

In this thesis I have thoroughly presented the current issues that the financial industry faces with expressing their risk profile, both internally and externally. The industry has expressed an increased will to focus on improving this practice after the financial crisis. This will to change the status quo is proved in both Ernst & Young's and in the survey from this thesis. The "only" problem that seems to remain is *how* this should be done. "Risk appetite" is currently the term that is most used for this purpose, but this thesis revealed in Part one that both the definitions and perceptions of the term are quite ambiguous and useless for its intended purpose. This led to the conclusion that "risk appetite" is a too narrow term to possibly explain the complex dynamics of a risk profile, and that it needs to be discarded in favor of two or three new terms.

Part two explored the opportunities of new terms throughout the financial industry and the petroleum industry and concluded with the use of RiskPAT as the replacement for the term "risk appetite". RiskPAT is a trio of the terms *risk preference*, *risk acceptance* and *risk tolerance* which through the concept works dynamically to optimize the communication of an organization's risk profile. In short, RiskPAT is a concept which makes it easier for the board to earn money by controlling risks, the core business of banking, by drastically improving the management of risk profiles. In addition, RiskPAT also works as an assurance of proper operational risk management to investors and bureaus, and indirectly benefits the organization by generally incentivizing forward-looking and pragmatic risk management.

The next chapter will present an example where RiskPAT is implemented and used to its full extent in a fictional bank, originally named Bank E.

4.2 Bank E's Implementation of RiskPAT

Bank E has, like the rest of the industry, realized that they need to focus on improving their current way their operational risk profile is communicated and controlled. Previously, they have tried to experiment with “risk appetite” without success, and have decided to implement RiskPAT instead.

4.2.1 Setting the risk preference and the risk acceptance

First of all, the board needs to state a general risk preference with a coherent risk acceptance for the whole organization. The board starts the whole process off by announcing an independent risk committee within the organization, which will be essential for the implementation of the RiskPAT. The committee and the board then discuss the risk profile that they ideally want, and state a *risk preference*, which reflects the preferred profile, and a *risk acceptance*, which is the allowed volatility of the preference. In Bank E's case it is the following statement: “*Bank E prefers to have an annual expected loss of \$25.000.000 on operational risks, but accepts a variance of 5%.*” After this stage is completed, the risk committee will continue the process by finding the *risk tolerance* of the organization and break down the risk preference to measurable objectives for each department.

4.2.2 Finding Bank E's risk tolerance

The risk tolerance is more of an objective value which is why only the risk committee is involved in the process of finding it. The risk committee thoroughly tests the external environment's tolerance of Bank E's operational risk management through scenario analyses and workshops, and reports the risk tolerance as: “*Bank E's risk tolerance is at an annual expected loss of \$40.000.000. If this limit is exceeded, Bank E will incur substantial losses due to lower ratings, which is considered intolerable.*” A graph which illustrates the RiskPAT can be seen in Figure 4.1.

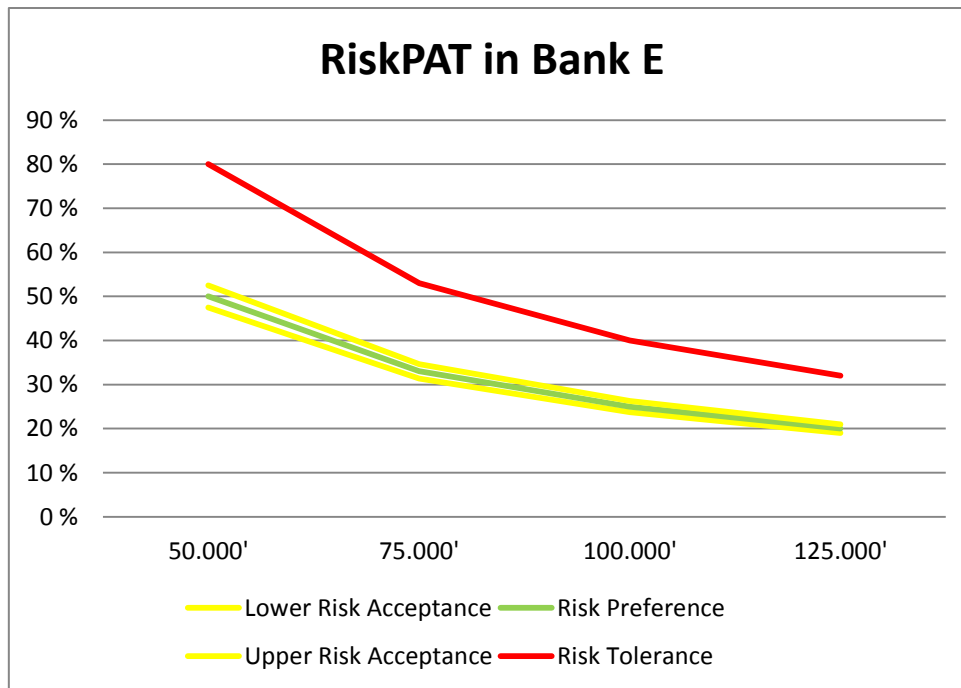


Figure 4.1 – RiskPAT in Bank E

The reason why the risk tolerance is found after the risk preference is purely a psychological choice made by Bank E. The board figured that the stated risk preference would be much more in line with the true state if it was unaware of the organization's risk tolerance. It is generally considered as detrimental if the risk preference exceeds the risk tolerance. If this was the case, and the board knew the risk tolerance, it would probably lead to a subconscious downward adjustment of the stated risk preference, which again would result in a biased result. Moving on, the next task for the risk committee is to optimize the conditions of communication by improving the internal environment.

4.2.3 Internal environment and risk identification

Bank E is AMA approved and is one, out of very few, that is currently using Bayesian network's for calculating the UL-part of their risk distribution. This further implies that the estimated operational risk exposure is properly reflected in the regulatory capital. Due to these conditions, Bank E has already identified and quantified most of their operational risks and also created individual distributions for all of these risks. This significantly decreases the workload of the risk committee, but they still have to thoroughly search the organization for additional unidentified risks. They manage to discover a previously undetected operational risk in the advisory department, which concerns the problem of advisor's giving wrong advices to clients. To assess this risk, the risk committee starts out by gathering expert opinions on the severity, probability and causes of the risk and some loss data from earlier

occurrences. With this data they estimate that the risk is mostly caused by aggressive incentives and a negative business culture. This information, along with the probabilities of each of them, is then plotted into a Bayesian network which helps to further develop the risk’s loss distribution (illustrated in Figure 4.2).

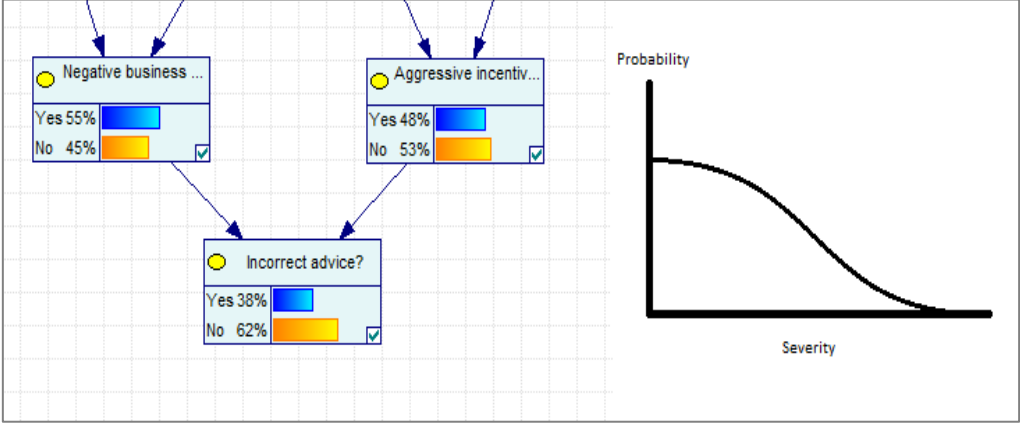


Figure 4.2 – Bayesian network and loss distribution of the risk of wrongly giving advice.

4.2.4 Breaking down the general risk preference

One of the most important challenges that the risk committee faces in this RiskPAT implementation is to break down the general risk preference into valid objectives for each department. Not only does the committee have to find a way to divide the overall preferred risk exposure throughout the divisions, they also have to make sure that all of the identified operational risks are reflected as well. The risk committee starts out by deciding that the best approach to divide the preferred risk exposure is by sharing it according to each department’s share of the whole organization’s VaR in an operational risk context. When it comes to making sure that all of the operational risks are covered, the committee finds that the best approach is to thoroughly make sure that all of the identified risks are covered. Some risks will naturally be spread over different departments and each of them will demand a different solution. It is therefore important that these are assessed and dealt with to avoid them being covered twice or not at all. The only way to do this is by being properly thorough when going through the risks.

After the risk preference is broken down, it needs to be compared to all of the different individual risk’s to check for its compliance. The risk profiles of the already identified risks are generally very compliant to the set risk preference within Bank E, but the newly discovered risk in the advisory department seems to be out of the risk preference’s bounds (illustrated in Figure 4.3).

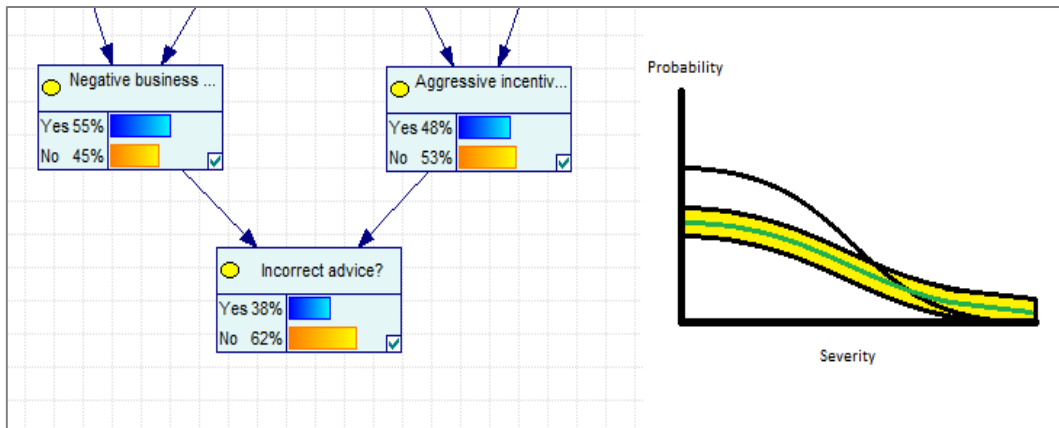


Figure 4.3 – The actual state of the operational risk (black line) compared with the risk preference (green line) and its surrounding risk acceptance (yellow zone)

This means that the risk probably will need mitigation, to comply with the risk preference, which will be done in collaboration with the board in the next stage.

4.2.5 Reporting and measuring compliance

When distributions have been made of all of the identified operational risks and all of the departments have received objectives which reflect the general risk preference, the risk committee’s direct role in the implementation of RiskPAT is almost over. The only remaining step is to communicate their discoveries and results to the board and assist with any urgent risk mitigation. The risk committee presents the risk tolerance together with the aforementioned risk that is currently incompliant with the risk preference. The board is not surprised by the stated risk tolerance of the organization, and is quite satisfied with the risk preference’s placement compared to it.

When it comes to the newly discovered operational risk in the advisory department, they decide that it needs to be mitigated to comply with the risk preference before publicly stating the RiskPAT. The risk committee presents the risk’s Bayesian network, and find that the most cost-efficient change they can make is to re-define the incentives to be less aggressive. The board initiates measures against the aggressive incentives, and one of the measures is against the current bonus criterion in the department. A monthly bonus qualification in the advisory department was earlier to: *“Get hundred or more clients to upgrade to a premium account.”* The board saw that this made the advisors suggest upgrades to all clients, including the ones that did not benefit on it and instead decided to close their account due to bad advisory. This made the board change the bonus qualification-objective to *“Get at least 70% of the clients that benefits from a premium account to upgrade.”* All of the registered upgrades also had to have the client’s individual benefits documented to avoid any advisors exploiting a loop-hole.

After assessing the aggressive incentives they find, through the risk’s Bayesian Network, that its loss distribution is perfectly compliant with the risk preference (illustrated in Figure 4.4).

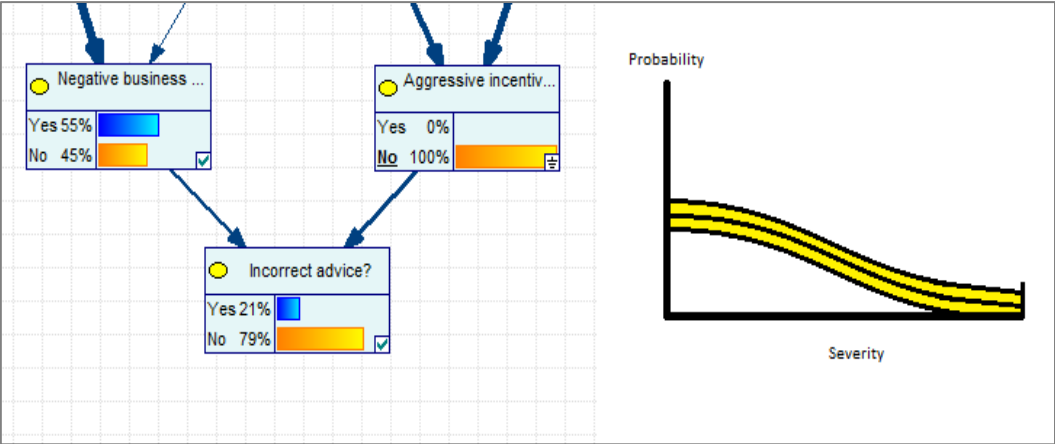


Figure 4.4 – The risk’s Bayesian network and loss distribution after the risk mitigation

After the board is up to date on the risk committee’s work, the committee is dissolved. The responsibility of following up and monitoring the risks, as well as the risk tolerance, will now be transferred to the risk department. The responsibility of ensuring that the risk preference at any time reflects the activity level of the organization is divided by between the board and the operational risk department. While the board ensures that the general risk preference is reflected by the activity level, the operational risk department ensures each department’s objectives stays in line with the general risk preference.

4.2.6 Publicly stating the RiskPAT and post-implementation benefits

The board of Bank E is now at a point where the RiskPAT has been stated and implemented. The adjustments to the urgent risks has also made the estimated risk preference to be within the stated risk acceptance zone, which further means that the RiskPAT is currently *valid* throughout Bank E. The board of Bank E is finally ready to publicly state the RiskPAT, which they choose to do in a press release.

Rating bureaus and potential investors now see Bank E as the superior bank in operational risk management compared to its competitors that do not have any way of properly expressing their risk profiles. The RiskPAT signals that Bank E has control and that it is open about sharing this. This increased transparency makes it easy for the rating bureaus and investors to understand how the bank operates (risk preference and risk acceptance) in terms of its limits (risk tolerance), which most likely will award Bank E with more capital through investments and increased rating. This would, naturally, be on behalf of other banks that have no proper

way of communicating their risk profile. These banks would have a harder time to acquire new investor's which would incentivize them to consider implementing RiskPAT as well.

4.3 Concluding Remarks and the Way Forward

This thesis has explored and mapped the status quo of risk profiles thoroughly. Many exiting discoveries throughout the thesis have ultimately led to the development of RiskPAT, which is my contribution to this area.

As demonstrated in this thesis, we see that RiskPAT is a tool that is made to be wielded by the board of a financial organization. If implemented and maintained correctly, it will significantly increase the control and the communication of an organization's risk profile. This will actively help the board with getting results by controlling risks, which is the core of the banking business. It is, however, important to remember that it still is a tool - not a miracle drug. RiskPAT cannot help the operational risk management if the conditions are poor; e.g. if the communication is in a prime state, while other processes are old and outdated. That is why this thesis has focused strongly on describing the internal environments that ideally should exist in the presence of RiskPAT.

There is much research that can be done to, further, enforce the concept of RiskPAT. The thesis has mentioned a few suggestions of subjects that could need more attention, such as seasonality in operational risk and KRI's that could make the BIA and the SA's estimated regulatory capital more reflected by the true risk exposure. Another subject that also could need attention is on finding methods for quantifying and measuring the loss of distinctive operational risks such as e.g. the temporary breakdown of an online banking service.

- Appendix -

Appendix 1: Definitions from M. Leitch's Article

| Source | Definition of "risk appetite" in 2009 |
|--|--|
| Institute of Internal Auditors | "The level of risk that an organization is willing to accept." |
| ISO Guide 73:2009 | "amount and type of risk that an organization is prepared to pursue, retain or take" |
| HM Treasury's Orange Book | "The amount of risk which is judged to be tolerable and justifiable" |
| Society of Actuaries | "the level of aggregate risk that an organization can undertake and successfully manage over an extended period of time." |
| COSO's ERM framework (2 definitions) | (1) "the degree of risk, on a broad-based level, that a company or other entity is willing to accept in pursuit of its goals." (2) "the amount of risk an entity is willing to accept in pursuit of value." |
| Business Continuity Institute | "The willingness of an organisation to accept a defined level of risk in order to conduct its business cost-effectively." |
| International Risk Management Institute | "The degree to which an organization's management is willing to accept the uncertainty of loss for a given risk when it has the option to pay a fixed sum to transfer that risk to an insurer." |
| Lloyds Market | "the willingness to take on risk" |
| Office of Government Commerce (OGC) | "An organization's unique attitude towards risk-taking which in turn dictates the amount of risk that it considers is acceptable." |
| Oxford Risk | "A person's propensity to prefer riskier or safer alternatives." |
| <i>"Risk Appetite: The Foundation of Enterprise Risk Management"</i> by Towers Perrin | "the total risk that an organization is willing to take to achieve its strategic objectives and meet its obligations to stakeholders." |
| <i>"What's your risk appetite?"</i> by Oliver Wyman | "the variability in results that an organization and its senior executives are prepared to accept in support of a stated strategy" |
| John Thirlwell in a presentation from 2007 | "the amount that a firm is willing to risk (for a given risk-reward ratio)" |
| Currency Financial Inc. | "The amount of capital that you are willing to lose in order to generate a potential profit." |
| Basel Committee, The FSA, The Financial Reporting Council, ACCA, AIRMIC and The IRM | Uses the term regularly but offer no definition |

Appendix 2: Survey Information

The questionnaire

The full version of the questionnaire can be found in the report in Appendix 3. It was constructed and distributed using the online service: QuestBack. It consists of 16 questions that contains, among other, multiple-choice questions, single select matrixes and free-text boxes. Everyone did not get the same questions due to some routing. I have made a routing map which is attached in the appendix (Appendix 4) to illustrate this better. The green boxes show which questions that was inquired given the answer to earlier questions. If the respondent was routed away from a question, the box is marked as red. With routing, the maximum number of questions that a respondent could be asked was fifteen, while the minimum number is six.

The first five questions (Q1-Q5) were aimed to get the respondents personal perception of the term “risk appetite” in the context of another term; “risk tolerance”. Three of these questions (Q2, Q3 and Q4) were free-text answers, while the other two (Q1 and Q5) was single-select questions. The next five questions (Q6-Q10) was more about the organizations risk strategy, and *its* use of the term “risk appetite”, while the final questions (Q11-Q16) was more aimed towards the organizations ambitions towards operational risk management. The very final question (Q16) was an open question which asks what the respondent perceives as the biggest barrier to operationalize the boards risk statement into the organization, which is answered by free-text.

The data

I got a respondent rate of 96% (22 banks out of 23), which is more than sufficient enough. The data was collected anonymously which makes this analysis indifferent to the specific banks attributes, which in other words mean that all answers are treated equally. Some of the collected data had to be edited due some errors in the questionnaire. All of the graphs and data in the report are unedited. The following remarks are about data that has been corrected with additional graphs in the appendix:

- Q5: 3 respondents answered “other”, which contains a free-text box. All of these answers could be placed throughout the scale (one in alternative two, one in alternative three and the last in alternative five. These adjustments shifted the average answer from 3,82 to 3,45. An adjusted graph can be found in Appendix 4.

- Q9 and Q10: A fault made by me during the production of the questionnaire slipped past the test phase in these questions. Question nine should either have contained an additional alternative which would have been “Both qualitative and quantitative”, or it should have been enabled for multiple choices. Seven of the respondents which chose alternative three; “Other”, stated that they used both methods. The way I have chosen to solve this is to add an adjusted graph with a third option “both qualitative and quantitative” in Appendix 4, and sorted all of the people that clearly stated that they used both into this option.
- Q10: This error in question nine directly contributed to only six respondents in question ten, due to routing. This erases some of questions ten statistical significance which means that it should be read for what they are worth. If this survey had been made for statistical analysis, the data should probably have been erased, but due to the qualitative nature of my survey, I have chosen to include them anyway. A side-note should be made that three of the respondents that answered alternative three; “Other”, in question nine, specifically mentioned how the operational risk profile is mentioned in the strategy. Two of these said that it was mentioned in qualitative terms, while the last one said that it was mentioned in quantitative terms. This is interesting since it to a certain degree proves the 33%-66% split, that the data already show.

The rest of the data is mostly consistent and needs no further commenting besides what is mentioned in the analysis.

Appendix 3: Survey Report

Studie om bruk av risikoappetitt

Publisert fra 16.04.2012 til 06.05.2012

22 respondenter (22 unike)

1. Hvordan kjenner du til begrepene risikotoleranse og risikoappetitt?



| Alternativer | Prosent | Verdi |
|---|---------|-------|
| 1 Jeg kjenner de som to begrep med forskjellig mening | 63,6 % | 14 |
| 2 Jeg kjenner de som synonymer | 31,8 % | 7 |
| 3 Jeg kjenner kun til risikotoleranse | 4,5 % | 1 |
| 4 Jeg kjenner kun til risikoappetitt | 0,0 % | 0 |
| 5 Jeg kjenner ikke til noen av begrepene | 0,0 % | 0 |
| Total | | 22 |

2. Vennligst beskriv hva du legger i ordet "risikoappetitt" kort med egne ord

Jeg oppfatter risikoappetitt som å "spekulere" i risiko i form av å få en gevinst av appetitten

Hvor stor risiko vi ønsker å ta innenfor de ulike risikoområdene

Jeg tolker det som et proaktivt begrep - hvor mye risiko ønsker jeg å ta

Den risiko vi er villig å påta oss.

Kort sagt i hvilken grad man har appetitt på risiko. Et statement om risikoappetitt skal gi en beskrivelse av villigheten til og overordnet rammeverk for å ta risiko.

Summen av risiko man er villig til å ta

Risikoappetitt er den risikoen virksomheten selv har satt som akseptabel risiko for sin eksponering innen ulike deler av forretningsvirksomheten. Altså summen av eksponering i eksempelvis kreditt området som er innenfor styringsmålet for kreditt til virksomheten. Tilsvarende for likviditetsrisiko, markedsrisiko etc

Risikoappetitt må forstås som en risiko som aktivt påtas med en forventning om risk adjusted return

Etter mitt syn vil risikoappetitt gjenspeile de strategisk valgene foretaket har lagt. Risikoappetitt gjenspeiles gjennom strategien.

Hvor mye kapital en virksomhet ønsker å eksponere for å nå et gitt forretningsmessig mål

Risikoappetitt er den risikoen man er villig til å ta innenfor en samlet risikokapasitet.

Viljen til å ta risiko

Risikoappetitt viser noe om hvilken grad av risiko banken er villig til å ta for øke sin verdi. F.eks å hente inn nye kunder.

Risikoappetitt er institusjonens vilje til risikotakning

3. Vennligst beskriv hva du vil legge i ordet "risikotoleranse" kort med egne ord

Jeg oppfatter risikotoleranse som et begrep for at man inser at det er noe risiko forbundet med det man gjør, men at dette er mer en akseptert risiko og ikke en spekulativ risiko

Hvor stor risiko vi tåler å ta ift bla kapitaldekning

Jeg tolker det som et mer reaktivt begrep - hvor mye risiko kan jeg ta (dvs ikke mer enn)

Mål på den totale akseptable risiko som banken eksponeres mot.

Den risiko som vi kan tåle i forbindelse med negative endringer.

Hvilken risiko tåler man å ta. Appetitten kan være lavere.

Punktet for risiko i hvert enkelt tilfelle som man lever godt med

Risikotoleranse er et kvantifisert mål på hvor stor eksponering for tap virksomheten i sum tåler sml med virksomhetens ansvarlige kapital. Sum risikoeksponering består av ulike beregnede eksponeringer i alle forretningsområder, og vil være større samlet enn hva risikotoleransen for tap ett år vil være. Altså sannsynlig tap ett år må være mindre enn hva virksomhetens risikotoleranse ifht kapitalens størrelse er.

Risikotoleranse (for operasjonell risiko) forstås som den risiko man er villig å akseptere hensyntatt marginalkostnad for reduksjon av (operasjonell) risiko (kalkulert risiko)

Risikotollerans går etter mitt syn mer på kombinasjon av eksponeringsnivå samt vurdert kvalitet på styring og kontroll av de ulike risikoene.

Hvor mye man tåler av svingninger i risiko

Risikotoleranse oppfatter jeg som en mer detaljert spesifisering av risikoappetitt for ulike risikoformer. F.eks. vil man være mindre tolerant ift. compliancerisiko.

toleevne for risiko

Risikoappetitt bør avgrenses av en risikotoleranse for å nå målet, m.a.o oppfatter jeg toleranse som en max grense på appetitten.

Det er institusjonens målramme for risikotagning

4. Hva legger du i disse begrepene (risikoappetitt/risikotoleranse)? Beskriv kort med egne ord.

Viljen til å ta på seg risiko. Rammer for eksponering. Fastsatt ved hjelp av tallfestede mål, evt. kvalitative faktorer i stedet for eller i tillegg til kvantitative mål. Har både overordnede appetitt-/toleransegrenser, samt mer nedbrytbare grenser.

konsernets definerte risikotoleranse grunnlaget for bankens holdning til risiko. Risikotoleranse (risikoappetitt) defineres som konsernets vilje til å påta seg risiko og fastsettes ved hjelp av relevante, overordnede og tallfestede mål så langt det er mulig. Fastssettelse av en risikotoleranse er en nødvendig forutsetning for å sette konsistente rammer for risiko og for å kunne systematisere et forsvarlig system for overvåkning av konsernets risiko. Styret fastsetter nivået på risikoappetitten gjennom risikostrategiene. I strategidokumentene definerer styret ønsket risikoprofil gjennom etablering av risikobaserte rammer og måltall på de ulike risikoområdene.

toleranse = maksimalgrense, appetitt = egentlig "lystnivå", men det eneste praktiske er å si at de to er synonymer i styringssammenheng

Risikoappetitt/risikotoleranse setter rammer for størrelse på ulike typer posisjonering. Er således førende for up-side og down-side. I bank representerer dette en vurdering av markeds-/resultatambisjoner sett opp mot finansiell og operasjonell kapasitet.

Begge begrepene anses å uttrykke hvor mye risiko man ønsker eller er villig til å ta på seg, hvor risiko uttrykker variasjonsrommet rundt forventet resultat. Samtidig som begrepene kan uttrykke det samme anses det mer naturlig å bruke appetitt i tilfeller hvor man har en reell oppsidedmulighet, og mer naturlig å bruke toleranse i tilfeller hvor man kun har nedsidevariasjon.

Jeg legger det samme i de to begrepene, altså vilje til å ta risiko.

Finansnæringen lever i stor grad av å ta kalkulert risiko. Disse begrepene mener jeg skal beskrive et nivå for hva som ansees som akseptabel risiko i forhold til forventede resultater/effekter.

5. Til hvilken grad brukes "risikoappetitt" og/eller "risikotoleranse" i det daglige i organisasjonen?



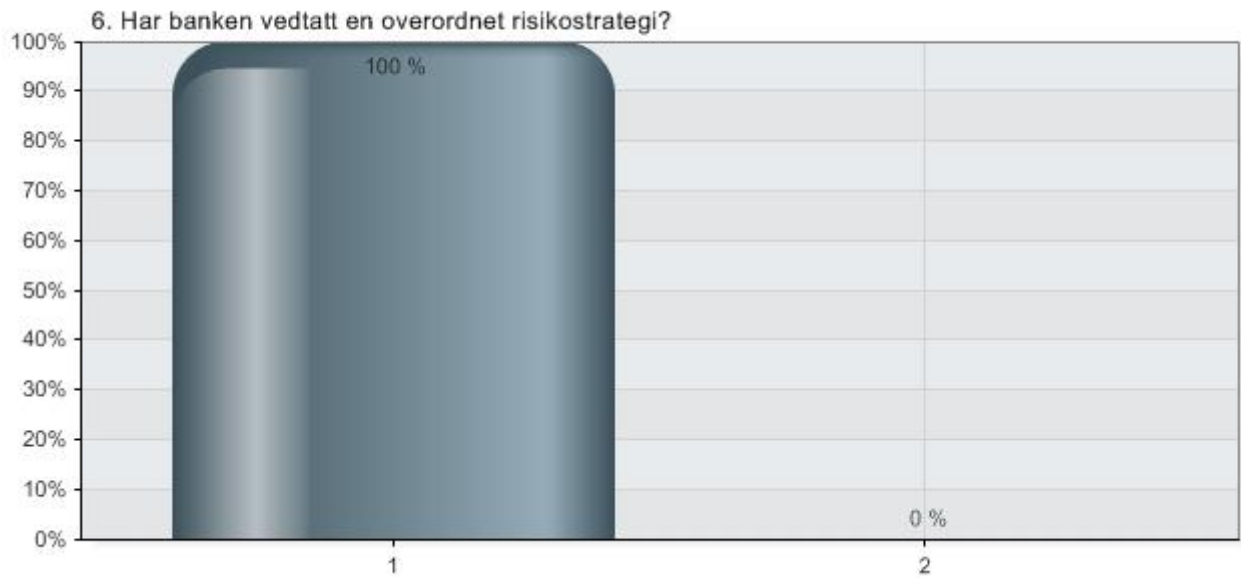
| Alternativer | Prosent | Verdi |
|------------------------|---------|-------|
| 1 Brukes ikke | 0,0 % | 0 |
| 2 I liten grad | 13,6 % | 3 |
| 3 I liten/middels grad | 31,8 % | 7 |
| 4 I middels/høy grad | 27,3 % | 6 |
| 5 I høy grad | 13,6 % | 3 |
| 6 Annet | 13,6 % | 3 |
| Total | | 22 |

I liten grad, men økende

I liten/middelsgrad, men dog allikevel implisitt i kredittarbeid

Risikoappetitt brukes ofte

6. Har banken vedtatt en overordnet risikostrategi?



| Alternativer | Prosent | Verdi |
|--------------|---------|-------|
| 1 Ja | 100,0 % | 22 |
| 2 Nei | 0,0 % | 0 |
| Total | | 22 |

7. Hvilke områder dekker den overordnede risikostrategien?



| Alternativer | Prosent | Verdi |
|-----------------------|---------|-------|
| 1 Kreditrisiko | 100,0 % | 22 |
| 2 Markedsrisiko | 100,0 % | 22 |
| 3 Operasjonell Risiko | 81,8 % | 18 |
| 4 Likviditetsrisiko | 95,5 % | 21 |
| 5 Andre risikoer | 68,2 % | 15 |
| -1 Vet ikke | 0,0 % | 0 |
| Total | | 22 |

Konsentrasjonsrisiko (både innenfor kreditt og andre risikoformer, samt mellom ulike risikoformer), forretningsrisiko, strategisk risiko,

omdømmerisiko

Risiko- og kapitalstrategi.

forretningsrisiko,compliancerisiko

eierrisiko, strategisk risiko, forretningsrisiko, omdømerisiko

Kapitalstrategi

Forretningsrisiko, strategisk risiko

strategisk risiko

Omdømme, konsentrasjonsrisiko, strategisk risiko, og forretningsrisiko

Konkrete styringsmål er knyttet til Kreditt, marked og likviditet. Alle risikoer og andre risikoer drøftes Q vis i ledergruppen, inkl evt tiltak.

Og operasjonell risiko er styrt gjennom risikobedømmingsprosess og intern kontroll system.

Konsentrasjonsrisiko

Operasjonell risiko (inkludert compliancerisiko)

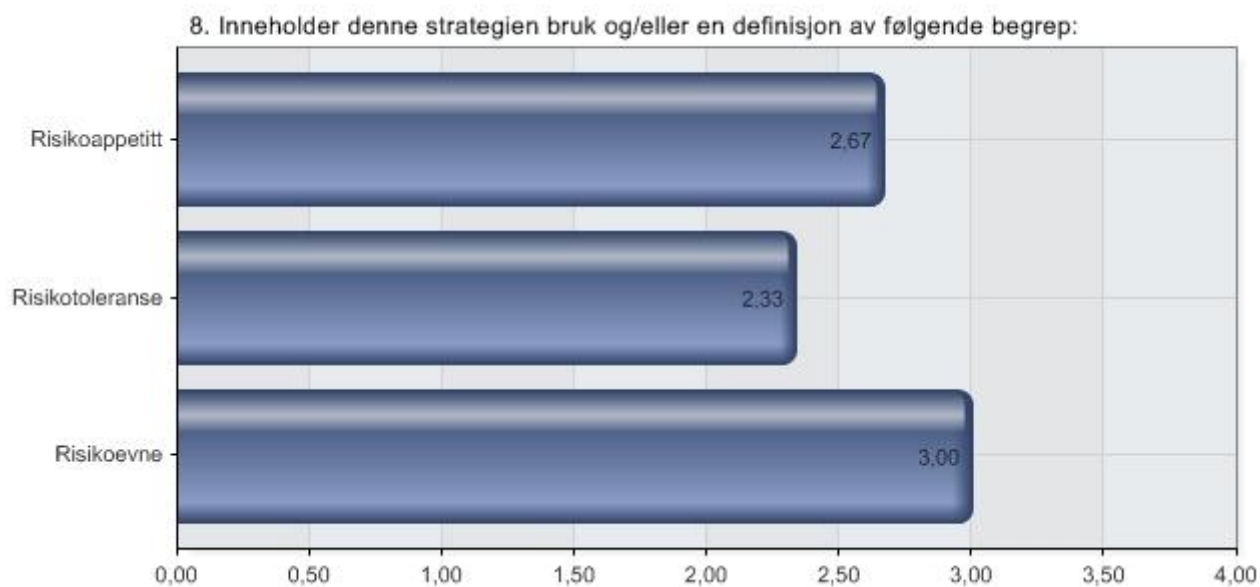
strategisk, omdømme

eierrisiko

Konsentrasjonsrisiko

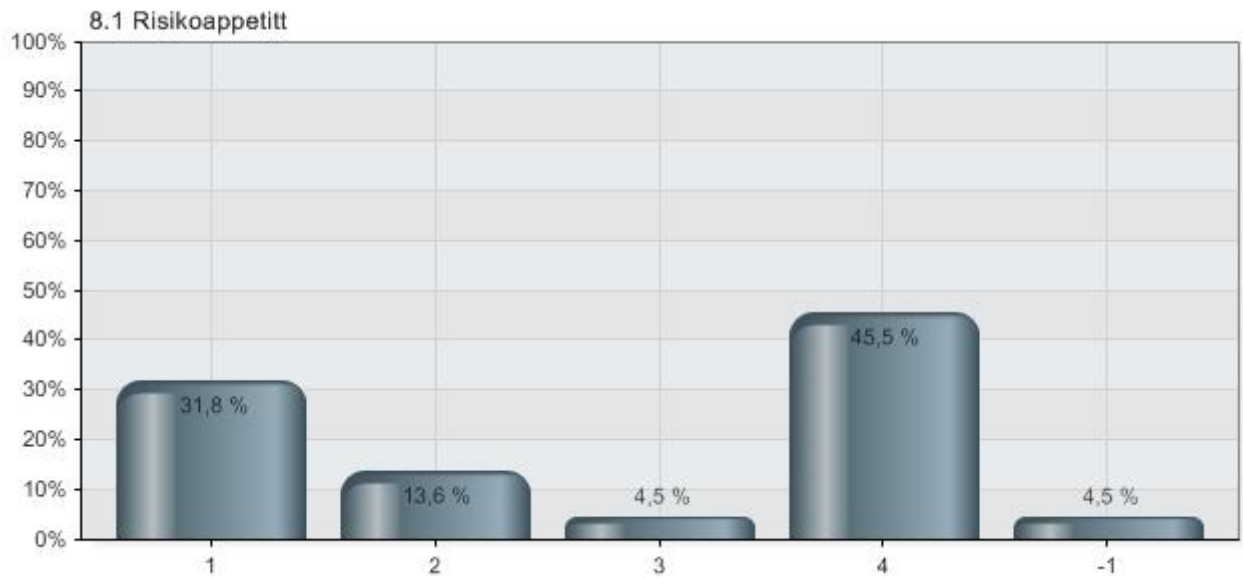
Forretningsrisiko (=strategisk risiko, omdømmerisiko og eierrisiko)

8. Inneholder denne strategien bruk og/eller en definisjon av følgende begrep:



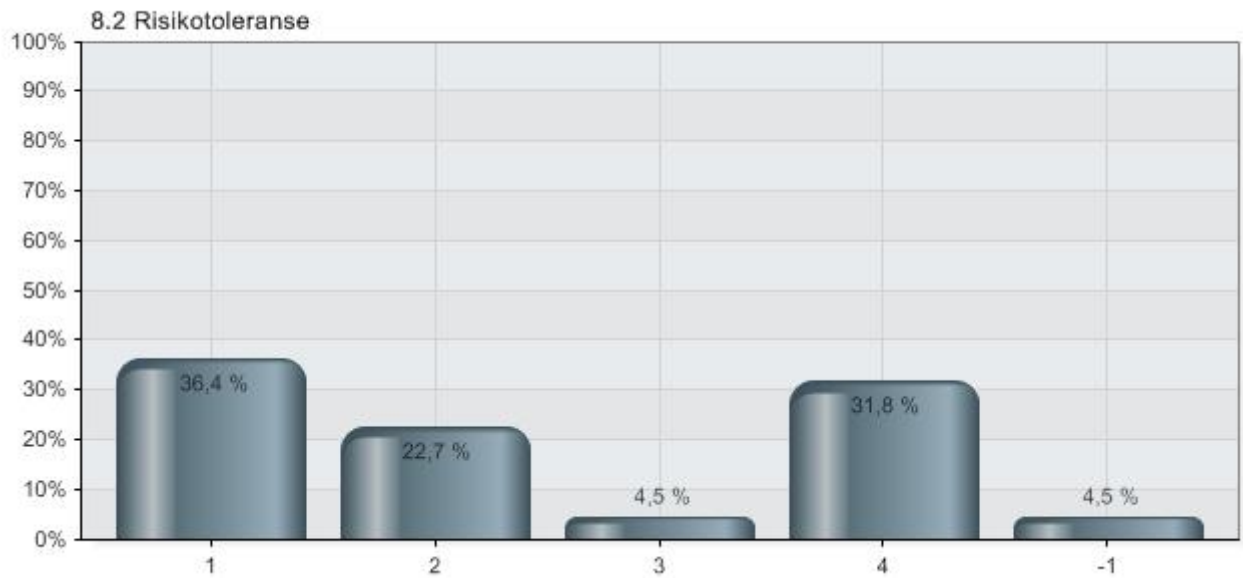
| Alternativer | N |
|-------------------|----|
| 1 Risikoappetitt | 22 |
| 2 Risikotoleranse | 22 |
| 3 Risikoevne | 22 |

8.1 Inneholder denne strategien bruk og/eller en definisjon av følgende begrep: - Risikoappetitt



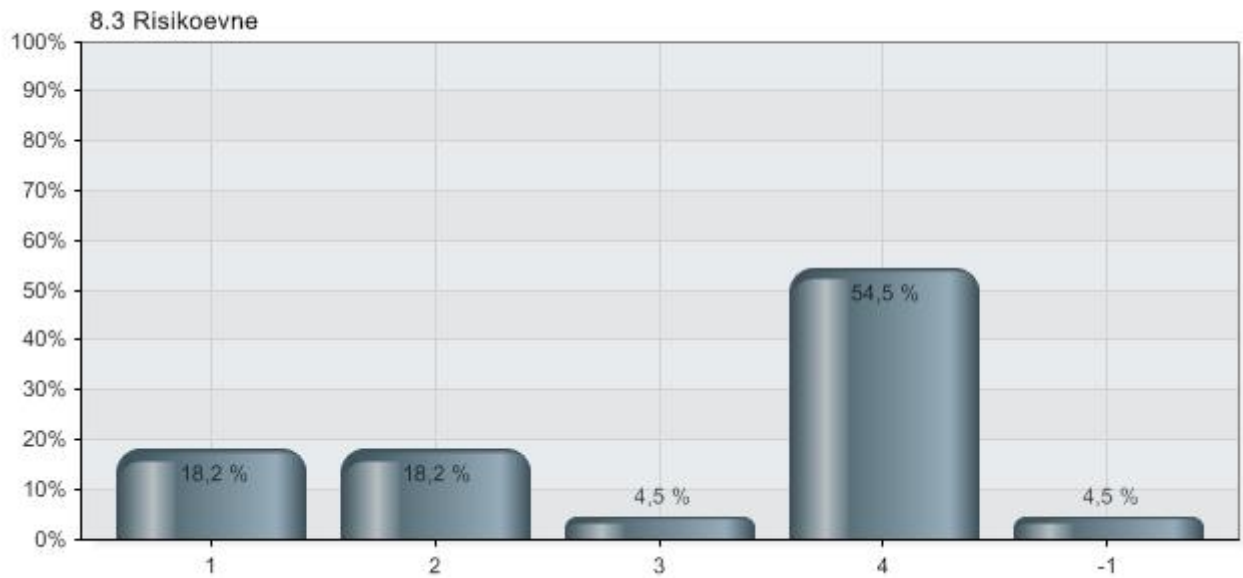
| Alternativer | Prosent | Verdi |
|---|---------|-------|
| 1 Ja, den bruker OG definerer begrepet | 31,8 % | 7 |
| 2 Ja, den bruker begrepet, men definerer det ikke | 13,6 % | 3 |
| 3 Ja, men kun en definisjon | 4,5 % | 1 |
| 4 Nei, den inneholder ikke begrepet | 45,5 % | 10 |
| -1 Vet ikke | 4,5 % | 1 |
| Total | | 22 |

8.2 Inneholder denne strategien bruk og/eller en definisjon av følgende begrep: - Risikotoleranse



| Alternativer | Prosent | Verdi |
|---|---------|-------|
| 1 Ja, den bruker OG definerer begrepet | 36,4 % | 8 |
| 2 Ja, den bruker begrepet, men definerer det ikke | 22,7 % | 5 |
| 3 Ja, men kun en definisjon | 4,5 % | 1 |
| 4 Nei, den inneholder ikke begrepet | 31,8 % | 7 |
| -1 Vet ikke | 4,5 % | 1 |
| Total | | 22 |

8.3 Inneholder denne strategien bruk og/eller en definisjon av følgende begrep: - Risikoevne



| Alternativer | Prosent | Verdi |
|---|---------|-------|
| 1 Ja, den bruker OG definerer begrepet | 18,2 % | 4 |
| 2 Ja, den bruker begrepet, men definerer det ikke | 18,2 % | 4 |
| 3 Ja, men kun en definisjon | 4,5 % | 1 |
| 4 Nei, den inneholder ikke begrepet | 54,5 % | 12 |
| -1 Vet ikke | 4,5 % | 1 |
| Total | | 22 |

9. Hvordan oppgis organisasjonens risikoprofil i strategien? (risikotoleransen/-appetitten/-evnen)?



| Alternativer | Prosent | Verdi |
|--|---------|-------|
| 1 Oppgis kvantitativt (f.eks. "Vi forventer et tap på 3 mill. og et maksimalt tap på 100 mill.") | 27,3 % | 6 |
| 2 Oppgis kvalitativt (f.eks. "Vi skal ha en lav operasjonell risiko") | 22,7 % | 5 |
| 3 Oppgis på annen måte | 50,0 % | 11 |
| Total | | 22 |

Den oppgis BÅDE kvantitativ og kvalitativ

Konsernets overordnede risikotoleranse skal være slik at det til enhver tid skal være 99,9 % sannsynlighet for at banken har tilstrekkelig kapital til å dekke uventede tap (økonomisk kapital). Økonomisk kapital beregnes over en tidshorisont på 1 år. kombinasjoner av de to første

Begge deler - kvalitativt og som ramme for risikjustert kapital

Oppgis såvel kvantitativt som kvalitativt. For op. risiko i hovedsak kvalitativt.

Den operasjonell oppgis kvalitativt. Mål for øvrige risikoer er knyttet til FTs moduler hvor vår organisering og styring ref til FTs beskrivelse av det nivå vi har valgt.

For op.risk= Statement + kvantifiserbar limit

Bruker kombinasjoner av stresstester og VaR

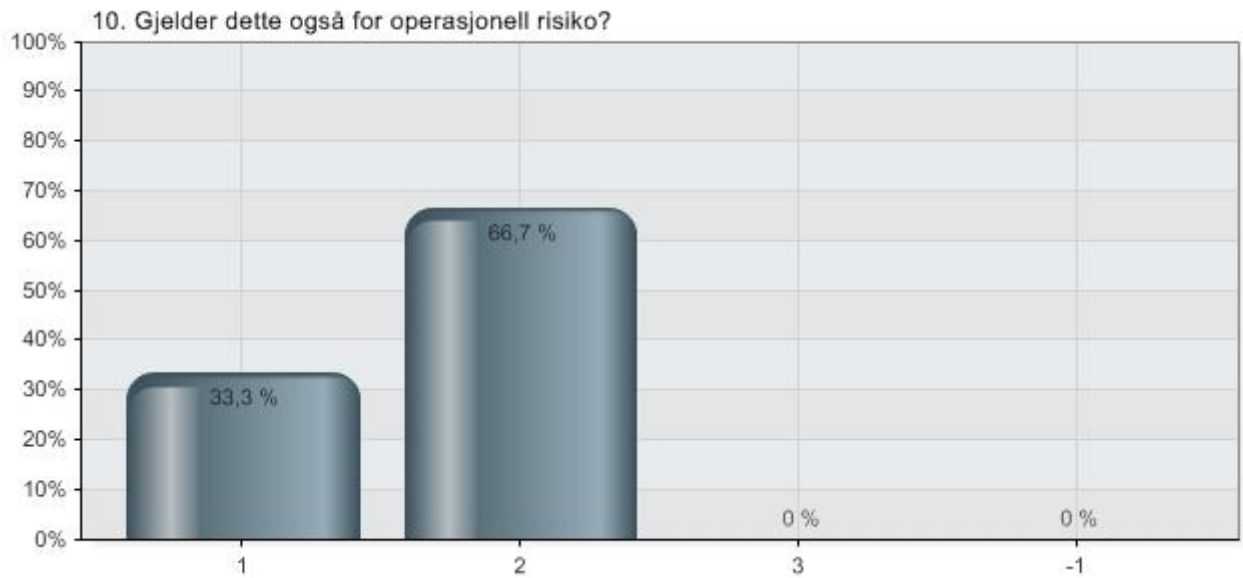
kvantitativt der det er relevant, men og kvalitativt for andre typer risiko

Både kvalitativt og kvantitativt

Både kvalitativt og kvantitativt, det kvalitative begrepet er ulikt kvantifisert innenfor ulike risikoområder på bakgrunn av antakelser om

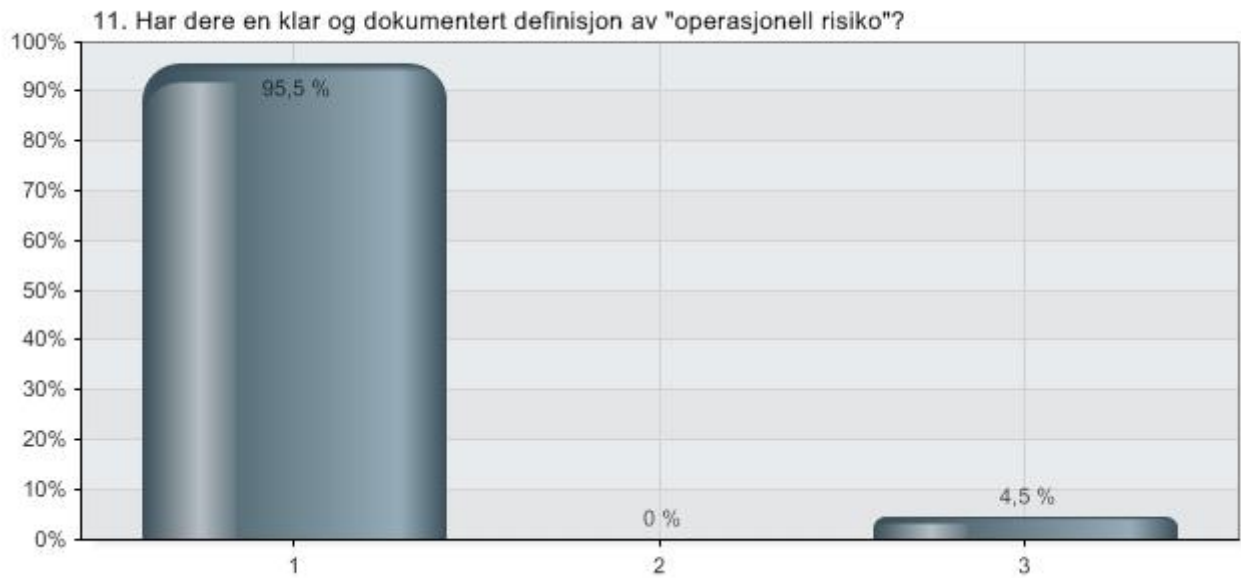
sannsynlighet og konsekvens.

10. Gjelder dette også for operasjonell risiko?



| Alternativer | Prosent | Verdi |
|--------------|---------|-------|
| 1 Ja | 33,3 % | 2 |
| 2 Nei | 66,7 % | 4 |
| 3 Annet | 0,0 % | 0 |
| -1 Vet ikke | 0,0 % | 0 |
| Total | | 6 |

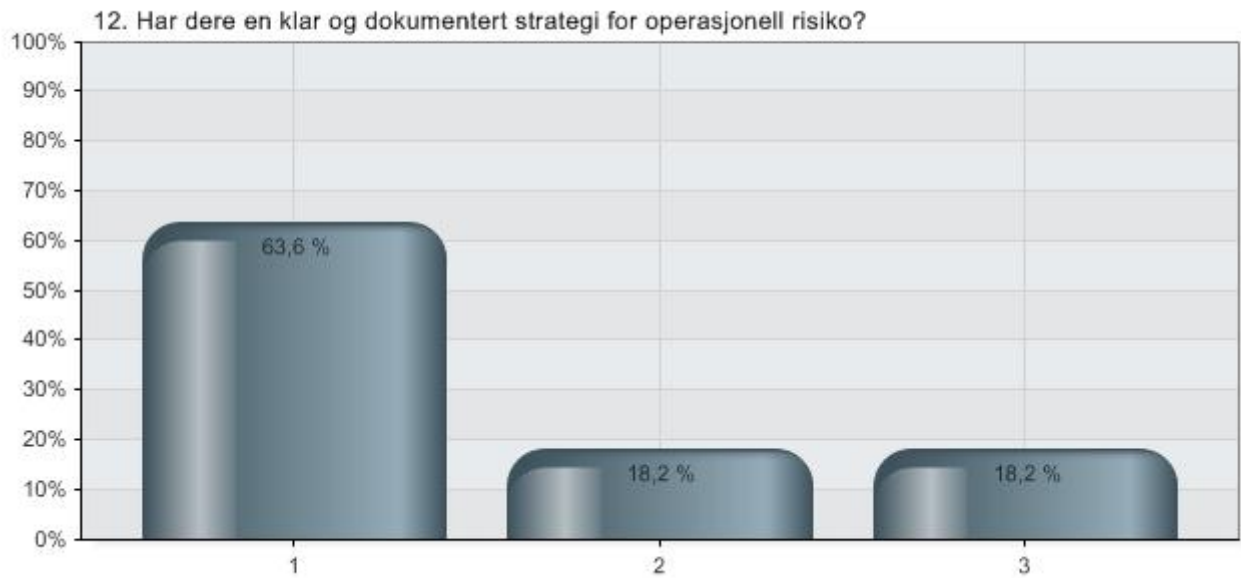
11. Har dere en klar og dokumentert definisjon av "operasjonell risiko"?



| Alternativer | Prosent | Verdi |
|--------------|---------|-------|
| 1 Ja | 95,5 % | 21 |
| 2 Nei | 0,0 % | 0 |
| 3 Annet | 4,5 % | 1 |
| Total | | 22 |

Ved bruk av historiske tall så er noen operasjonell risiko inkludert, Basel 2 vil ta større hensyn til operasjonell risiko

12. Har dere en klar og dokumentert strategi for operasjonell risiko?



| Alternativer | Prosent | Verdi |
|--------------|---------|-------|
| 1 Ja | 63,6 % | 14 |
| 2 Nei | 18,2 % | 4 |
| 3 Annet | 18,2 % | 4 |
| Total | | 22 |

Ingen strategi, men en policy er under arbeid

Vi har en strategi/policy for operasjonell risiko. Denne skal imidlertid bli tydeligere og dokumenteres bedre. Ja i form av Basel 2 implementering 2014

13. Til hvilken grad er denne risikostrategien operasjonalisert i organisasjonen?



| Alternativer | Prosent | Verdi |
|---------------------------|---------|-------|
| 1 Ikke operasjonalisert | 0,0 % | 0 |
| 2 Delvis operasjonalisert | 35,7 % | 5 |
| 3 Fullt operasjonalisert | 64,3 % | 9 |
| 4 Annet | 0,0 % | 0 |
| Total | | 14 |

14. Hvor mange operasjonelle risikoer har banken identifisert?



| Alternativer | Prosent | Verdi |
|--|---------|-------|
| 1 Over 50 risikoer | 13,6 % | 3 |
| 2 10-50 risikoer | 54,5 % | 12 |
| 3 Under 10 | 4,5 % | 1 |
| 4 Det er ikke identifisert noen risikoer | 9,1 % | 2 |
| 5 Annet | 18,2 % | 4 |
| Total | | 22 |

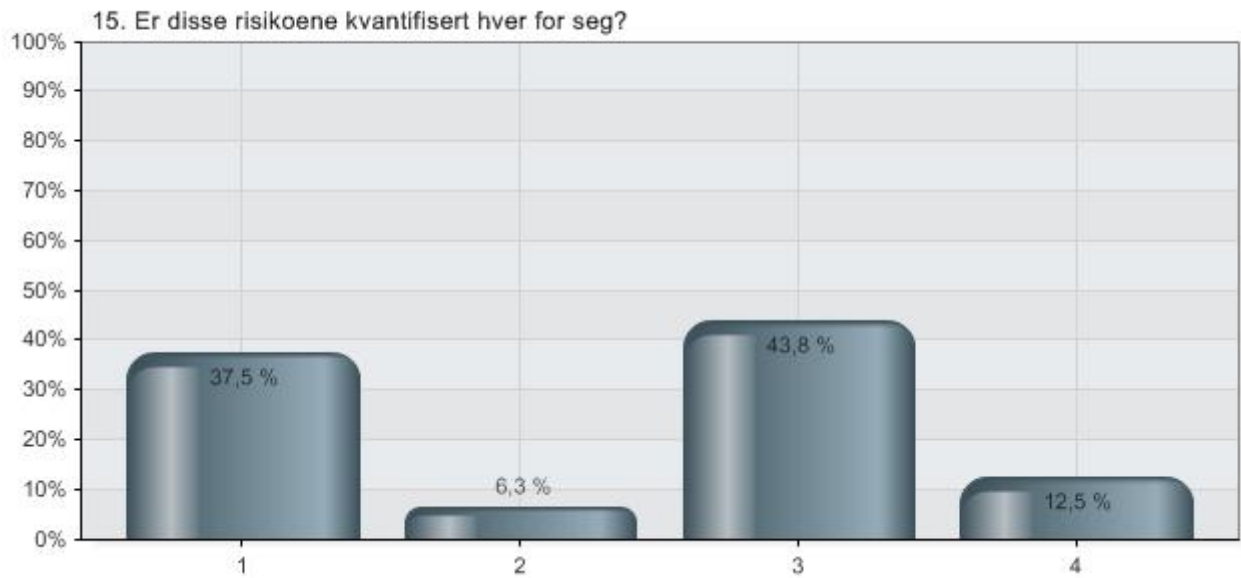
7 stykk ut fra AMA-metode, samt omdømme, forr.risiko og strat.risiko (de tre siste kan sees på som en del av op.risk)

Identifisert mange, men ingen samlet totaloversikt

Ikke tallfestet - risikobildet oppdateres løpende.

Det har jeg ikke oversikt over her

15. Er disse risikoene kvantifisert hver for seg?



| Alternativer | Prosent | Verdi |
|--|---------|-------|
| 1 Ja, som poeng (f.eks. sannsynlighet 3 x konsekvens 4 = 12 poeng) | 37,5 % | 6 |
| 2 Ja, som hele beløp (f.eks. forventet tap 3 mill. og maksimalt tap 100 mill.) | 6,3 % | 1 |
| 3 Nei | 43,8 % | 7 |
| 4 Annet | 12,5 % | 2 |
| Total | | 16 |

De fleste som beløp - alle er ikke mulig å kvantifisere i beløp

De antatt største risikoen tildeles risikoverdi

16. Hva anser du som den største barrieren for å bli bedre på å implementere styrets ønskede risikonivå inn i den daglige risikostyringen?

Stadig mer komplekst og skiftende regelverk, etterlevelse og fokus i organisasjonen i en ellers travel hverdag for den enkelte, tidsriktig oppfølgingssystem

kommunikasjon og forståelse i organisasjonen

Prioritering av tid og ressurser i linjen - til kontroll, tiltak og utvikling

Når det gjelder operasjonell risiko mangler vi gode modeller/måleverktøy for å kartlegge risikoen. Barrieren ligger også tilstrekkelig med fokus hos operative ledere

forretningsforståelse

Det var et stort spørsmål, men den første utfordringen er å oversette en kvalitativ målsetting om f.eks moderat risiko til en kvantitativ størrelse

Kompetanse, eierskap, forståelse av risikostyring som ledd i verdiskapingen.

--

Helhetlig forståelse av risiko.

Manglende kompetanse/forståelse av fordelene ved å bruke ressurser på det.

Systemer og rutiner som sikrer korte kommunikasjonsveier og læringsløyper i organisasjonen slik at endringer i risikobildet raskt kan vurderes og nødvendige tilpasninger kan utføres.

At styret selv er kompetent til å vurdere forskjellige risikonivåer

elektronisk Risiko , I k og compliance system, fleksibelt ifht redigering endring av både risikobedømminger og som et resultat av kvantifisert sannynlighet og konsekvens- justering av nødvendige nøkkelkontroller for å bringe operasjonell risiko ned på akseptabelt nivå. Gjerne web basert pga behov for å lett tilgang og lett administrasjon.

Holdninger, systemer

Utfordrende å tildele risikotoleranse til (relevante) prosesser, samt å sikre felles "måleenhet" i virksomheten på noe som ofte oppleves som "kvalitativt".

Operasjonalisering av risikostyring i driften av virksomheten.

Det må oppleves som verdiskapende for brukeren (gulrot) og få negativ konsekvens ved svikt (pisk)

Å finne relevante, kvantitative indikatorer, som er enkelt å beregne.

Betre og meir effektive rapporteringssystem

For svake ledelsesinformasjonssystemer, mange fagsystemer, ressursbruk, implementering på de laveste nivåene av organisasjonshierarkiet.

Det krever høye kostnader og mye system utvikling for å levere i henhold til kravene for styre og Basel. Nødvendig men krevende og den største utfordringen.

Det vil byråkratisere banken ytterligere

Appendix 4: Survey Routing Map

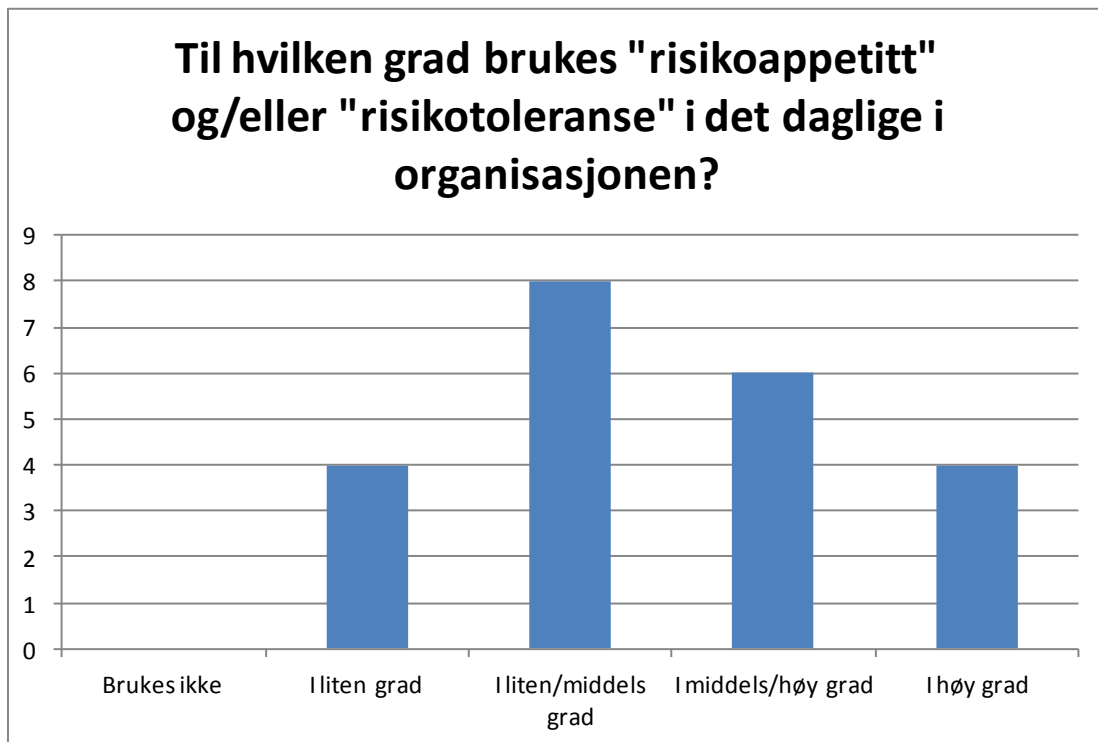
| Question 1 | Question 2 | Question 3 | Question 4 | Question 5 | Question 6 | Question 7 | Question 8 |
|---------------------------------|------------|------------|------------|------------|--|------------|------------|
| Alt. 1: Q2, Q3 and Q5 before Q6 | | | | | Alt. 1: Q7, Q8, Q9 and possibly Q10 before Q11 | | |
| Alt. 2: Q4 and Q5 before Q6 | | | | | | | |
| Alt. 3: Q3 and Q5 before Q6 | | | | | Alt. 2: Straight to Q11 | | |
| Alt. 4: Q2 and Q5 before Q6 | | | | | | | |
| Alt. 5: Straight to Q6 | | | | | | | |

Routing map 1 - Question 1-8

| Question 9 | Question 10 | Question 11 | Question 12 | Question 13 | Question 14 | Question 15 | Question 16 |
|------------------------------|-------------|-----------------|------------------------------|-------------|--------------------------------|-------------|-------------|
| Alt. 1: Q10 before Q11 | | All alt. to Q12 | Alt. 1: Q13 before Q14 | | Alt. 1, 2 or 3: Q15 before Q16 | | |
| Alt. 2 or 3: Straight to Q11 | | | Alt. 2 or 3: Straight to Q14 | | Alt. 4 or 5: Straight to Q16 | | |
| | | | | | | | |

Routing map 2 - Question 9-16

Appendix 5: Adjusted Graphs



Graph 1 - Question 5 adjusted graph, new average answer = 3,45



Graph 2 - Question 9 adjusted graph

References

- Finansdepartementet. (2007). Om forvaltningen av Statens pensjonsfond i 2007. Available: <http://www.regjeringen.no/nb/dep/fin/dok/regpubl/stmeld/2007-2008/stmeld-nr-16-2007-2008-/5.html?id=505818>. Last accessed 20th Feb 2012.
- Øystein Olsen. (2011). En verdensøkonomi i endring. Available: <http://www.norges-bank.no/no/om/publisert/foredrag-og-taler/2011/31052011-en-verdensokonomi-i-endring/>. Last accessed 21st Feb 2012.
- Aamo, B.S. and Bellamy, A.M. (2009). Veiledning til forskrift om risikostyring og internkontroll. Available: <http://www.finanstilsynet.no/no/Artikkelarkiv/Rundskriv/2009/1-kvartal/Veiledning-til-forskrift-om-risikostyring-og-internkontroll/>. Last accessed 21st Feb 2012.
- COSO. (2004). Enterprise Risk Management — Integrated Framework. Available: http://www.coso.org/documents/coso_erm_executivesummary.pdf. Last accessed 21st Feb 2012.
- COSO. (2012). Understanding and Communicating Risk Appetite. Available: http://www.coso.org/documents/ERM-Understanding%20%20Communicating%20Risk%20Appetite-WEB_FINAL_r9.pdf. Last accessed 22nd Feb 2012.
- Institute of Risk Management. (2011). Risk Appetite & Tolerance Guidance Paper. Available: <http://www.theirm.org/publications/documents/IRMRiskAppetiteFullweb.pdf>. Last accessed 19th Mar 2012.
- Matthew Leitch. (2010). Risk appetite definitions. Available: <http://www.internalcontrolsdesign.co.uk/appetitedef/index.shtml>. Last accessed 17th Feb 2012.
- Norges Største Bedrifter. (2011). Rangeringsliste for "Bank". Available: <http://www.norgesstorstebedrifter.no/bransjeliste/770/>. Last accessed 17th Apr 2012.
- Euromoney Magazine. (1996). December issue. Unknown author.
- Basel Committee on Banking Supervision. (2001). Operational Risk. Available: <http://www.bis.org/publ/bcbsca07.pdf>. Last accessed 23rd Apr 2012.
- Tattham, David (2011). A Short Guide to Operational Risk. Great Britain: Gower Publishing Company. 13-14.

- David Häger (2011). Course: Operational Risk Management, Lecture no. 2: Måling av operasjonell risiko. Universitetet i Stavanger.
- ORX. (2012). About ORX. Available: <http://www.orx.org/about-orx>. Last accessed 26th Apr 2012.
- Terje Aven and Jan Erik Vinnem (2007). Risk Management - With applications from the Offshore Petroleum Industry. London: Springer. 49-67.
- Basel Committee on Banking Supervision. (2005). Part 2: The First Pillar — Minimum Capital Requirements. Available: <http://www.bis.org/publ/bcbs118b.pdf>. Last accessed 11th of May 2012.
- Lasse B. Andersen. (2011). Course: Operational Risk Management, Lecture no. 1: Introduction to operational risk management. Universitetet i Stavanger.
- Dictionary.com. (2012). Tolerate. Available: <http://dictionary.reference.com/browse/tolerate>. Last accessed 22nd May 2012.
- The Institute of Operational Risk. (Dec. 2009). Risk Appetite. Sound Practice Guidance.
- Frode Bø (2012). Presentation: Styling av operasjonell risiko. Risk Forum 2012. 19. januar 2012.
- E&Y (2011). Ernst & Young. Presentation: Trender internasjonalt i Risk Management. 5. oktober, Stavanger
- Basel Committee on Banking Supervision. (2003). Sound Practices for the Management and Supervision of Operational Risk. Available: <http://www.bis.org/publ/bcbs96.pdf>. Last accessed 6th Jun 2012.
- Investopedia. (2012). Financial Distress Definition. Available: http://www.investopedia.com/terms/f/financial_distress.asp. Last accessed 8th Jun 2012.
- Dagens Næringsliv. (2009-2012). Acta Kapitalforvaltning. Available: <http://www.dn.no/sok/?q=Acta+Kapitalforvaltning&type=dn>. Last accessed 8th Jun 2012.
- Dagens Næringsliv. (2007). Terra Securities ferdig. Available: <http://www.dn.no/forsiden/naringsliv/article1249754.ece>. Last accessed 8th Jun 2012.

