Universiteit Leiden
Opleiding Informatica

The IT aspect of Operational Risk

Name: Zoi Ralli
Studentnr: s1274023

Date: 19/08/2014

1st supervisor: Dr. Stefan Pickl
2nd supervisor: Dr. H.T. Le Fever

MASTER'S THESIS

Leiden Institute of Advanced Computer Science (LIACS)
Leiden University
Niels Bohrweg 1
2333 CA Leiden
The Netherlands

Contents

1 Introduction **11**

2 Methods **13**

3 Types of Risk & Definitions **14**
3.1 Early Definitions of Risk . . . 14
3.2 Risk as Defined after 1990 . . . 15
3.2.1 General Definitions of Risk . . . 15
3.2.2 Risk Defined by Public Organizations & Institutions . . . 16
3.2.3 The Engineering Approach to Risk . . . 18
3.2.4 Medical Risk . . . 19
3.2.5 Economy & Risk . . . 19
3.2.6 An Anthropology Perspective of Risk . . . 19
3.2.7 Political Risk . . . 19
3.2.8 Financial Risk . . . 21
3.2.9 Supply Risk . . . 22
3.2.10 IT Risk . . . 22
3.2.11 Fiduciary Risk . . . 22
3.3 Working Definition . . . 23

4 The IT Aspect of Operational Risk **24**
4.1 Operational Risk . . . 24
4.1.1 About Operational Risk . . . 24
4.1.2 Operational Risk Management . . . 33
4.2 IT Risk . . . 36
4.2.1 About IT Risk . . . 37
4.2.2 IT Risk Management . . . 42

5 Case Study **48**
5.1 Experiment Motivation and Description . . . 48
5.2 Results . . . 52
5.3 Secondary Observations . . . 56

6 Conclusion **62**

7 Discussion **63**

A Post-Experiment Document **65**

B Insightly Interface **68**

C Experiment Results **70**

List of Tables

1 Risk characteristics and corresponding definitions[8] . . . 16
2 Risk characteristics and corresponding definitions [48] . . . 16
3 Cultural prototypes and their reaction to Risk [5] . . . 20
4 Categories of Country Risk . . . 20
5 Event types of Operational Risk according to Basel II . . . 27
6 Business lines according to Basel II . . . 27
7 Threat metrics by class . . . 30
8 National and international ORM standards and guidelines (as found in [2]) . . . 36
9 Professional ORM standards and guidelines (as found in [2]) . . . 37
10 Operational Risks that connect to IT systems and their usage (as extracted from [17]) . . . 39
11 Overview of risk-reducing measures (as found in [9]) . . . 47
12 Sex, age, academic level and field of studies information of the Test Group . . . 50
13 Minimum, maximum and average total completion time and number of errors of the *Trained* Group . . . 52
14 Minimum, maximum and average total completion time and number of errors of the *Untrained* Group . . . 53
15 Comparison of the two groups' average time per task and average number of errors . . . 54
16 Types of errors, in which task they were recorded and how many times in total (Frequency), and per group (Frequency Trained, Frequency Untrained) . . . 56
17 Female and Male subgroups, how many members they include, their average total completion time and number of errors . . . 57

List of Figures

1 What Operational Risk includes (as found in [29]) . . . 25
2 A generic classification scheme about causes and effects of Operational Risk (as found in [45]) . . . 31
3 The position of Operational Risk in an enterprise (as found in [52]) . . . 32
4 The cycle of Operational Risk Management (as found in [29]) . . . 34
5 IT as value enabler, inhibitor or destructor (as found in [20]) . . . 41
6 Three levels approach to IT Risk Management (as found in [9]) . . . 46
7 The homepage of "Insightly" . . . 51
8 Time spent on each task per *Trained* user . . . 53
9 Time spent on each task per *Untrained* user . . . 54
10 Total time spent per *Trained* and *Untrained* user sorted from minimum to maximum . . . 55
11 Total time spent per *Trained* and *Untrained* Femaleuser, both mixed (upper graph) and sorted from minimum to maximum (lower graph) . . . 58
12 Total time spent per *Trained* and *Untrained* Maleuser, both mixed (upper graph) and sorted from minimum to maximum (lower graph) . . . 59
13 Total time spent per *Trained Female* and *Trained Male* user sorted from minimum to maximum . . . 59
14 Total time spent per *Untrained Female* and *Untrained Male* user sorted from minimum to maximum . . . 60
15 Total time spent per *Female* and *Male* user sorted from minimum to maximum 60
16 Level of computer skills among the users that performed zero (0) errors . . . 61

Executive Summary

Nowadays, risk is a main issue of concern for every organization and this is reinforced by the wide deployment of Information Technology. Risk is present in many functions and internal operations of each organization, referred as Operational Risk during the recent years. In this document, Operational Risk is explained in detail, following a presentation of not only generic risk, but also of how risk is perceived in a variety of different areas. Afterwards, risks related to Information Technology operations are further described and guidelines on IT Risk Management are introduced. Attention is drawn on the risks created by failures caused by employees' inadequate knowledge on how to use enterprise software. Lack of training is claimed to be one of the main reasons for this and this is evaluated by the conduction of an experiment under which two groups of people use a piece of software with and without training. The results indeed show that employee training on new software before it is deployed can improve their effectiveness and consequently decrease Operational Risk, provided that no alterations take place in the company and its environment.

1 Introduction

The term "Risk", which nowadays is present in every organization, derives from the early Italian word "riscare" which means "to dare" [14]. Taking risks has been always inherent in humans [57], and as a consequence it was introduced in every aspect of human life where decisions have to be taken. Its presence became apparent in science and in the business world, thus official efforts to define, evaluate, control and face Risk took place. The following stage was the formation of various frameworks and guidelines in order to assess and regulate risk, and at present most organizations have special teams or even departments responsible for examining and managing risk.

Due to the variety of fields that the concept of risk applies to, numerous types of risk have been identified in the literature. They will be presented and defined in this thesis, giving an overall perspective of the concept. More specifically, Chapter 3 touches upon multiple definitions of Risk, following the thesis Introduction (Chapter 1) and the methods that will be used for the research (Chapter 2).

Thereupon and as the business environment, services and processes have become more complex [49], and the number of failures in businesses' operations is rising, one of the most recently established type of Risk, namely Operational Risk, is becoming of increasing significance. Hence this thesis regards Operational Risk, which incurs mainly from failures in the organization's internal processes [10]. As the term is still not mature enough, academic research on it still needs to be done on some of its abundant aspects [37]. In particular, due to the fact that it was initially established for financial institutions, most of the existing literature examines Operational Risk in regards to this approach. However, in the meantime Information Technology (IT) systems and software have become indispensable not only for financial organizations but for business entities of all types, rendering Operational Risk as a concern of vital importance for every organization since its drivers for both financial and non-financial organizations are the same [47]. In this thesis, Operational Risk is viewed in the scope of organizations of all types regarding the aspect of IT, the risks that may incur by IT software and services, as well as the possible relationship that exists between Operational Risk and IT Risk, which is presented in Chapter 4. More specifically, the term "Operational Risk" and some well-known guidelines are described in Chapter 4.1, followed by a presentation of IT risks as a subsection of Operational Risk in Chapter 4.2.

While reviewing the literature, it was concluded that IT systems are a common source of operational failures which add up to an organization's total amount of Operational Risk [45]. One of the main reasons for this is the fact that employees do not get sufficient training and therefore they do not have adequate knowledge of using the software ([30], [45]). This fact led us to build the Research Question: "Does employee training on a new software improve its usage so as to reduce Operational Risk?".
An experiment will be set up in this context in order to examine whether training improves the way people use a new piece of software. The software that will be used is a Customer Relationship Management (CRM) software for Small and Medium Enterprises (SMEs). Thirty (30) participants will be randomly divided into two (2) groups of fifteen (15) people. All of them will be asked to perform the same specific guided tasks using the software, but the one group will go through training prior to this. While performing the tasks, both group members'

activities will be recorded by special software. In addition, the participants will be asked to fill in a questionnaire after the conduction of the experiment in order to acquire additional data. The participants' behaviour while using the software is going to be measured in terms of efficiency and effectiveness by measuring the time they need to complete specific tasks, and comparing the number of errors that were observed between the two (2) groups.

The specific software was selected since CRM systems are one of the most widely used types of software in enterprises ([28], [50]), and since no other experiment about training on CRM software was found in the literature. In addition, no experiment was found in the literature that examined training of software in terms of both efficiency and effectiveness. Although experiments that test training in terms of only effectiveness like in [40] or only efficiency like in [51] do exist, an experiment that analysed training on IT software and more specifically a CRM system, regarding both aspects was not found in the literature. Thereupon, the fact that both efficiency and effectiveness are going to be measured in order to evaluate the groups of the users makes the experiment complete and well-justified. Therefore, the experiment will be set up in a way that it can be linked with the employees of a company that use a software and whether undergoing training can decrease the level of Operational Risk caused by failures and errors in IT systems.

2 Methods

Initially, literature review was conducted to analyse Risk in its generic sense. Articles and research papers were reviewed to identify and define the various types of Risk. The databases of Leiden University, Universität der Bundeswehr München and Google Scholar were browsed with "Risk" as the key search term. The following step was backward search of the articles that were of relevance, in order to include many different aspects of Risk. After recognizing the main types of Risk, a search was performed for each of them, with each type of Risk as the key search term (e.g. "Political Risk", "Medical Risk" etc.). When appropriate, backward search was conducted again.

Afterwards, the same procedure was followed but more specifically for Operational Risk and its IT aspect. The key search terms used were "Operational Risk" and "Operational Risk Management" in combination with "IT Risk", "IT Risk Management" and "technology". The search was performed in the aforementioned databases as well as in the IEEE Xplore Digital Library. Although in the previous stage no time limit was set, in this step articles that were written mostly after 2000 were selected. Backward search was once more performed, and eventually the review of the literature led us to the formation of a Research Question.

In order to acquire an answer to the Research Question, an experiment was performed. Thirty (30) participants used a software, and they were split into two groups. Everyone performed the same given tasks and their actions were monitored, but the one group received training prior to this. Specific metrics and measurements were taken for every user, which were finally compared between the two (2) groups. The experiment is explained and analysed in detail in Chapter 5.

3 Types of Risk & Definitions

This chapter is an introduction to the term Risk. A number of definitions are reviewed in order for the reader to get acquainted with the term and the alternative meanings it can acquire according to the fields within which it is defined.

When reviewing the existing literature on the topic, it was observed that from the academic articles and books found, the ones which were published before 1990 defined risk in a more broad and subjective way. Nevertheless, in the more recent literature (after 1990) that was reviewed, more concrete definitions were established.

Therefore, this chapter is divided into two main sections: chapter 3.1 refers to definitions of risk before 1990 and chapter 3.2 to the ones after 1990. Chapter 3.2 arranges definitions in groups and presents risk according to various fields of science; namely: general definitions of risk, risk defined by public organizations & institutions, the engineering approach to risk, medical risk, economy & risk, an anthropology perspective of risk, political risk, financial risk, supply risk, IT-related risk and fiduciary risk. In the last part of the chapter, section 3.3 will present the definition that is chosen to be used in the rest of this thesis.

3.1 Early Definitions of Risk

Risk is an equivocal term and it can be defined in a variety of different ways according to the context that surrounds it. During the first academic attempts to define risk that were before 1990, it had a more generic meaning which could be adapted to the concerning field of interest ([8], [21], [27]) . Due to this effort to cover the meaning of risk universally, the "subjectivity" and "uncertainty" of risk were main characteristics of the proposed definitions. Thus users could adapt the definitions in their field of interest and specify the term's aspects according to their goals, sometimes even intuitively [21]. As Kaplan and Garrick proposed, "risk is not objective; it is relative to the observer" [27]. As a result, there was not only one definition of risk that was agreed upon by everyone because a definition that is appropriate for all possible problems and circumstances was not considered to be feasible. Rather, each definition should envisage one's perspective and concern on the various outcomes and their consequences on a particular problem, in order to evaluate the tradeoffs between loss and profit incurred by risks. [21].

These facts can be summarized in the following definitions. The first one defines the concept of a risk in a descriptive way, the second one is a qualitative definition and the last one is a quantitative definition:

1. "If the distinction between reality and possibility is accepted, the term risk denotes the possibility that an undesirable state of reality (adverse effects) may occur as a result of natural events or human activities. This definition implies that humans can and will make causal connections between actions (or events) and their effects, and that undesirable effects can be avoided or mitigated if the causal events or actions are avoided or modified. Risk is therefore both a descriptive and a normative concept. The definition of risk contains three elements: undesirable outcomes, possibility of occurrence, and state of reality" [42].

2. Risk = uncertainty + damage [27]

3. The Risk, **R**, is the set of triplets:

$$R = (s_i, p_i, xi), i = 1, 2, ..., N \quad (1)$$

where:

$\mathbf{s_i}$ is a scenario identification or description

$\mathbf{p_i}$ is the probability of that scenario

$\mathbf{x_i}$ is the consequence or evaluation measure of that scenario, i.e. the measure of damage [27]

It was in the next decade that risk started to get defined in a more concrete way and have a specific and different meaning according to the environment within which it was developed. Definitions of risk in regards to a number of areas are presented in the following section, starting with a general approach and proceeding to definitions within more and more specific areas of expertise.

3.2 Risk as Defined after 1990

3.2.1 General Definitions of Risk

There exist a lot of general definitions of risk which are abstract enough to be adjusted in a variety of different cases. In this group of definitions, the terms "uncertainty", "outcome", "consequence" and "human value" are in common, as it can be observed:

- "Risk results from the direct and indirect adverse *consequences* of *outcomes* and events that were not accounted for. It involves (i) consequences, (ii) their probabilities and their distribution, (iii) individual preferences and (iv) collective, market and sharing effects" [55].

- "Risk is a situation or event where something of *human value* (including human themselves) is at stake and where the *outcome* is *uncertain*" [43], [44].

- "Risk is an uncertain *consequence* of an event or an activity with respect to something that *humans value*" [4].

- "Risk is equal to the two-dimensional combination of events/*consequences* and associated *uncertainties*" [6].

- "Risk is *uncertainty* about and severity of the *consequences* (or *outcomes*) of an activity with respect to something that *humans value*" [4].

- "Risk is the extent to which there is *uncertainty* about whether potentially significant and/or disappointing *outcomes* of decisions will be realized" [53]. Inherent in this definition are the dimensions of *outcome uncertainty*, *outcome expectations* and *outcome potential* [58].

Risk Characteristics	Definition
Variability of returns	Firm performance evaluated in terms of return and growth criteria
Variance	Variability of the probability distribution of returns
Market Risk	The use of the capital asset pricing model to measure risk (Capital Asset Pricing Model)
Risk as innovation	Risk conditions equated with conditions characterized by newness, uncertainty, and lack of information
Risk as entrepreneurship	Independence of action in venturing into the unknown
Risk as disaster	Strategies that could result in corporate disaster, bankruptcy or ruin
Accounting risk measures	Accounting ratios related to risk of ruin, default or bankruptcy

Table 1: Risk characteristics and corresponding definitions[8]

- "Risk is the combination of probability and extent of *consequences*" [3].

Moreover, Baird and Thomas [8] and Shapira [48] give a different definition of risk depending on its characteristics, which are presented in Table 1 and Table 2 respectively.

Risk Characteristics	Definition
Downside of risk	Risk being associated with a negative outcome
Magnitude of possible losses	At least one possible outcome of an uncertain situation having a bad outcome
Distinction between risk taking and gambling	Risk taking is associated with using skills, judgement, and control, while gambling is not
Risk as a multi-faceted construct	Risk cannot be captured with a single number, since multiple facets such as financial, technical, marketing, production and other risk aspects exist

Table 2: Risk characteristics and corresponding definitions [48]

3.2.2 Risk Defined by Public Organizations & Institutions

It is common that public organizations and institutions make their own effort in defining risk. These definitions can be generic or concerning more specific types of risk, depending on the type, the activity field and the goal of each organization. These efforts aim to standardization

of the risk terminology, in order to create definitions that are unanimously accepted and widely used, on a national or even a global level.

To begin with, according to Standards Australia [1] risk is "the chance of something happening that will have an impact upon objectives. It is measured in terms of consequences and likelihood." Similarly, UK Government explains risk as "the uncertainty of outcome, whether positive opportunity or negative threat, of actions and events. It is the combination of likelihood and impact, including perceived importance" [2]. Moreover, as stated by the US Presidential/Congressional Commission on Risk Assessment and Risk Management [3] and the World Health Organization [4], risk is "the probability of a specific outcome, generally adverse, given a particular set of circumstances" and "a probability of an adverse outcome, or a factor that raises this probability", respectively. Most of the aforementioned definitions can be summed up in the following one which is provided by the US Nuclear Regulatory Commission [5] "The combined answers to (1) What can go wrong? (2) How likely is it? and (3) What are the consequences?"

Risk definitions by institutions which point out the aspect of expected losses in various fields were found. More specifically, the United Nations International Strategy for Disaster Reduction [6] describe risk as "the probability of harmful consequences, or expected losses (death, injuries, property, livelihoods, economic activity disrupted or environment damaged) resulting from the interactions between natural or human-induced hazards and vulnerable conditions", whereas the definition given by the European Environment Agency [7] is "expected losses (of lives, persons injured, property damaged and economic activity disrupted) due to a particular hazard for a given area and reference period. Based on mathematical calculations, risk is the product of hazard and vulnerability".

The German Advisory Council on Global Change [8] defines risk taking into account several

[1] Standards Australia is Australia's non-government standards organisation. Risk is defined in the document "Risk management - Principles and guidelines (AS/NZS ISO 31000:2009) (http://www.standards.org.au/)

[2] UK Government defines risk in the Handling Risk Report with title "Communicating Risk Guidance"

[3] The US Presidential/Congressional Commission on Risk Assessment and Risk Management was a commission authorized as part of the Clean Air Act Amendments of 1990 to perform risk assessment. Risk is defined in the document "Framework for Environmental Health Risk Management". (http://www.riskworld.com/riskcommission/default.html)

[4] World Health Organization (WHO) is the regulatory authority for health within the United Nations. Risk is defined in the document "The World Health Report 2002: Reducing Risks, Promoting Healthy Life". (http://www.who.int/)

[5] The United States Nuclear Regulatory Commission (U.S.NRC) aims to achieve nuclear safety for the people and the environment in the U.S. Risk is defined in U.S.NRC online glossary (http://www.nrc.gov/reading-rm/basic-ref/glossary/full-text.html), (www.nrc.gov/)

[6] The United Nations International Strategy for Disaster Reduction (UNISDR) is the office responsible to coordinate disaster risk reduction activities within the United Nations (UN). Risk is defined in the document "Living with Risk: A global review of disaster reduction initiatives, 2004-Version 1". (http://www.unisdr.org/)

[7] The European Environment Agency (EEA) is focused to provide information about the environment within the European Union. Risk is defined in the EEA online glossary (http://glossary.eea.europa.eu/), (www.eea.europa.eu/)

[8] The German Advisory Council on Global Change (WBGU) is the body responsible for analysing global environment and global change. (http://www.wbgu.de/)

angles of the term, such as technical, social and socio-economic and differentiating the definition for each one of them. Thus, risk is explained as follows: "In a technical perspective, risk refers to two variables the probability of occurrence of a specific instance of damage and the extent of that damage. The social science perspective focuses on aspects of societal and psychological risk experience and risk perception, while socio-economic approaches focus on risks to livelihood, security and the satisfaction of basic needs".

It is interesting to also point out some views towards risk from more exquisite perspectives, that is how risk is considered when related to atomic energy or chemical safety. The International Atomic Energy Agency [9] interprets risk as "a multi-attribute quantity expressing hazard, danger or chance of harmful or injurious consequences associated with actual or potential exposures which relates to quantities such as the probability that specific deleterious consequences may arise and the magnitude and character of such consequences". Moreover, under the International Programme on Chemical Safety [10], risk is viewed as "the probability of an adverse effect in an organism, system or (sub) population caused under specified circumstances by exposure to an agent".

3.2.3 The Engineering Approach to Risk

The Engineering approach to risk is also interesting and worth to be pointed out. It can be distinguished to the traditional engineering approach and the Bayesian approach. The former can be classified as a positivist view, i.e. risk exists objectively in the world and thus it can be measured. On the other hand, the latter proposes that risk is "a way of expressing uncertainty". This point of view expresses a more balanced way to define risk between the two extremes (positivism and relativism), and is the more suitable version for analyzing risk on a practical basis [5]. More specifically, as Aven and Kristensen [5] propose:

i The traditional approach to risk and risk analysis is based on the idea that risk exists objectively and the risk analysts see the analyses as a tool for producing estimates of this objective risk

ii The Bayesian approach proposes that risk is primarily a judgement, not a fact. As risk expresses uncertainty about the world, i.e. about consequences and outcomes of an activity, risk perception has a role to play to guide decision makers.

No matter the approach that is chosen, in an engineering context risk includes the following components:

- A: what can go wrong
- C: the consequences of these events in case they occur
- P: the probabilities of A and C

So, risk can be described as $R = (A, C, P)$ [4].

[9] The International Atomic Energy Agency (IAEA) is the world's center of cooperation in the nuclear field. Risk is defined in IAEA online glossary (http://www.iaea.org/)

[10] Through the International Programme on Chemical Safety (ICPS), the World Health Organization (WHO) aims to establish the scientific basis for the sound management of chemicals. Risk is defined in the document "Principles and Methods for the Risk Assessment of Chemicals in Food, Chapter 2: Risk Assessment and its role in Risk Analysis"

3.2.4 Medical Risk

From a health perspective, medical risk is viewed in regards to physical safety. Therefore it can be defined as an "an exposure to the chance of injury or financial loss" [56]. Another definition of risk regarding health issues is provided by the Food and Agriculture Organization of the United Nations which describes risk as "the likelihood of the occurrence and the likely magnitude of the consequences of an adverse event to animal or human health in the importing country during a specified time period" [11]. Moreover, the Codex Alimentarius Commission defines risk as "a function of the probability of an adverse health effect and the severity of that effect, consequential to a hazard(s) in food" [12]. Additionally, the International Atomic Energy Agency [13] views risk as "the probability of a specific health effect occurring in a person or group as a result of exposure to radiation".

3.2.5 Economy & Risk

In the area of economics, the definition of risk is viewed as a judgement about uncertainty. This judgement can vary from an objective statistical probability to a subjective probability that evaluates the degree of belief and the related uncertainties. This perspective has also been widely used in psychology [5]. Shifting to the area of econometrics, Cool defines risk as the "absolute value of probable loss" [56].

3.2.6 An Anthropology Perspective of Risk

In this field, risk is examined from the perspective of how individuals respond to risk. It is viewed in terms of how can different cultures, pattern behaviours and perceptions influence the way individuals react and interact with risk [5]. As an example, one of the most popular models which identifies five typical cultural prototypes is presented below in Table 3.

3.2.7 Political Risk

Sethi and Luther [46] define political risk as:

i "Unanticipated government actions that have an impact on business operations. National governments by their actions might prevent business transactions, change terms of agreements or even expropriate business units".

ii "The other definition is on the basis of environmental changes due to political developments (like acts of violence, instability, riots and so on) that have repercussions on business activity". Here it can be added that events which arise from authority, power relationships or even sociocultural developments (e.g. violent government changes, growing national pride on the ownership of businesses) can also provoke political risk.

[11] Food and Agriculture Organization of the United Nations (FAO) is focused on achieving food security for all. The FAO Emergency Prevention System (EMPRES) Animal Health provides a risk definition in the document "Risk Analysis and OIE". (http://www.fao.org/home/en/)

[12] Codex Alimentarius Commission is focused on international standards for the safety and quality of international food trade. It provides a risk definition in the document "Guidance for Governments on Prioritizing Hazards in Feed" (www.codexalimentarius.org/)

[13] The International Atomic Energy Agency (IAEA) is the world's center of cooperation in the nuclear field. Risk is defined in IAEA online glossary (http://www.iaea.org/)

Cultural Prototypes	Reaction to Risk
Entrepreneur(individualistic)	The market rules. Risks offer opportunities and should be accepted in exchange for benefits.
Egalitarian	Risks should be avoided unless they are inevitable to protect the public good.
Bureaucrat	Risks are acceptable as long as institutions have the routines to control them.
Atomised or stratified individuals	Life is a lottery. Risks are out of our control: safety is a matter of luck.
Autonomous individuals (The Hermit)	Risks are acceptable as long as they do not involve coercion of others.

Table 3: Cultural prototypes and their reaction to Risk [5]

These two definitions are interdependent and the two types of events that provoke risk (governmental or environmental) are not mutually exclusive, which means that they can happen simultaneously, or also the one can provoke the other to happen. Political risk can affect any business entity in a different way than market developments. The harshness of the potential effect and the vulnerability level of a company to political risk depend on the country, the industry or business sector and the firms characteristics [46]. This is why in the field of politics and political risk, the term "country risk" is also often encountered when the interest is on international business transactions and not on domestic ones. Geographic location along with economic structures, currency, culture and sociopolitical characteristics shape the risk for each country. Country Risk Analysis attempts to analyze and eventually decrease the risks of cross-border investments, taking also into consideration the growing imbalances that could possibly harm the return on investment. In fact, D. Meldrum in his paper "Country Risk and Foreign Direct Investment" [35] presents six categories of country risk where economic and political risk lie among them:

Categories of Country Risk
Economic Risk
Transfer Risk
Exchange Rate Risk
Location of Neighborhood Risk
Sovereign Risk
Political Risk

Table 4: Categories of Country Risk

3.2.8 Financial Risk

Financial risk refers to possible losses in financial markets. Shifts of financial variables like interest and exchange rates may generate risk for almost every corporation [23]. As a result, in the financial sector, risk has an important role in decision making and nowadays it is common for every financial institution to have a department specialized in risk management. The main types of risk that are distinguished in this field are:

Credit Risk

Credit Risk emerges when counterparties are not willing or able to pay off their legitimate or agreed obligations. It leads to losses when debtors are downgraded by their creditors or credit agencies, which results in a decline of the market value of what they owe. Credit risk can be measured as the cost of the cash flow that is needed in order to replace the counterparty's contribution that was not fulfilled [23]. The original definition created by the Basel Committee on Banking Supervision is: "The extension of loans is the primary activity of most banks. Lending activities require banks to make judgements related to the creditworthiness of borrowers. These judgements do not always prove to be accurate and the creditworthiness of a borrower may decline over time due to various factors. Consequently, a major risk that banks face is credit risk or the failure of a counterparty to perform according to a contractual arrangement. This risk applies not only to loans but to other on- and off- balance sheet exposures such as guarantees, acceptances and securities investments" [10].

Market Risk

Market Risk emerges when there are variations in the prices of assets and liabilities. Based on the asset or liability type, four categories of market risk can be identified: *interest rate risk, equity risk, foreign exchange risk* and *commodity risk* [23]. The original definition created by the Basel Committee on Banking Supervision is: "The risk of losses in on and off-balance sheet positions arising from movements in market prices" [10].

Liquidity Risk

Liquidity risk can appear in two forms: market product liquidity risk and funding risk. The first type of liquidity risk arises when transactions cannot be carried out due to inadequate market activity, whereas the latter appears when a business entity is unable to fulfil its cash flow obligations and thus is forced to proceed to early liquidation actions, converting "paper losses" into actual losses [23].

Operational Risk

Operational Risk, which is the most recently identified type of risk in the financial sector, is defined by the Basel Committee on Banking Supervision as: "the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk" [10]. Although this was the first official definition given to Operational Risk and was widely used since then by academics, it has also been claimed that because the term is very recent, there does not exist a definition that is universally acknowledged, and that in many cases each company creates its own [37]. Indicatively, some of them interpret it as the total risk that remains when market and credit risk are removed, or as the risks that incur from after transaction clearing and settlement procedures [37]. A definition from a broad perspective

describes Operational Risk as the risk created by an operational failure [45]. Moreover, it has also been defined as "the risk that is related to the bank's operations and how a failure in an operational safeguard could impact the stability of the bank" [33]. Finally, according to Gaese, "Operational Risk refers to potential losses resulting from inadequate systems, management failure, faulty controls, human error or fraud" [23].

3.2.9 Supply Risk

Risk is found to have acquired a particular position in supply chain management and logistics. Thus "supply risk" is defined as:

i "The probability of an incident associated with inbound supply from individual supplier failures or the supply market occurring, in which its outcomes result in the inability of the purchasing firm to meet customer demand or cause threats to customer life and safety" [58].

ii "The transpiration of significant and/or disappointing failures with inbound goods and service" [58].

iii "The risk that adversely affects inward flow of any type of resource to enable operations to take place" [36].

3.2.10 IT Risk

With regards to Information Technology (IT), IT Risk is defined as "every business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterpsrise. IT Risk (also seen as Technology Risk) consists of IT-related events that could potentially impact the business. It is characterized by both uncertain frequency and magnitude, and it creates challenges in meeting strategic goals and objecives as well as uncertainty in the pursuit of opportunities" ([11], [13], [19]). Or, as defined in [17] "Technology Risk includes the failure to respond to sophisticated client requirements, market and regulatory changes and evolving internal needs for information and knowledge management, as well as many other issues such as:human error; internal fraud through software manipulation; external fraud by intruders; obsolescence in applications and machines; reliability issues, mismanagement; and the effect of natural disasters". In other words, IT risk refers to the business risk that is developed by the use of IT. IT Risk is neither exclusively about IT Security Risk, nor is a merely technical issue. On the contrary, it contains all aspects of Information and Technology risk and the benefits or threats they may bring about [26]. For example, one subcategory of IT Risk can be the risk incurred in the management of computer data centres, which is defined as "risk considered in terms of security of the physical system and data and service disruption in the management of computer data centres" [56].

3.2.11 Fiduciary Risk

Fiduciary risk is a type of risk that can be encountered in enterprises that advertise a product that differs to the one that they actually offer. This is not considered to be an action of fraud, but it may lead to massive product recalls that will harm significantly the reputation of the company and its relationship with customers [39].

3.3 Working Definition

In this document the term "Risk" will refer to "Operational Risk: the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk.", as introduced by the Basel Committee on Banking Supervision. This is selected as the working definition of this document because the focus of the research is on Operational Risk. This definition serves as the most appropriate for Operational Risk as it was the first official effort to define this particular type of risk. Furthermore, although it comes from the financial industry of banks, it is seen that it is acknowledged also in the academic world. It is widely used in scientific papers, and some subsequent efforts to define Operational Risk are mainly based on this definition, while trying to extend or enrich it.

Moreover, from Chapter 4.2 and on, the term "IT Risk" will also be introduced and analysed. This term is defined by ISACA [14] as "every business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterpsrise. IT Risk consists of IT-related events that could potentially impact the business. It is characterized by both uncertain frequency and magnitude, and it creates challenges in meeting strategic goals and objecives as well as uncertainty in the pursuit of opportunities".

[14]Information Systems Audit and Control Association (ISACA) is an independent, non-profit, global association which engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems

4 The IT Aspect of Operational Risk

This Chapter is divided into two (2) sections. Section 4.1 focuses on Operational Risk and section 4.2 on IT Risk. In both sections, there are two (2) parts: the first serves as an introduction in each topic and the latter presents well know frameworks about Operational Risk Management and IT Risk Management, respectively.

4.1 Operational Risk

4.1.1 About Operational Risk

History

Operational risk emerged in the end of the 1960s after the manufacturing industry faced problems of delivery delays as a result of mass production and too many products and services offered [16]. However,it was not until the early 1990s that Operational Risk and its management became more common, more specifically after the collapse of Barings Bank in 1995 [15] ([16], [39]). Due to this and also to the fact that the term was officially defined for the first time in 1999 in the Basel II Accord by the Basel Committee on Banking Supervision, Operational Risk is closely related with financial institutions. In the beginning, all risks confronted by financial institutions that could not be quantified constituted the Operational Risk that the institution was facing [18]. So the addition of Operational Risk in the Accord was considered to be quite innovative at the time because only Credit and Market risk were counted for estimating the total risk that a financial institution was facing [33]. Nevertheless, Operational Risk, more than Credit or Market risk, is not limited to banking and financial institutions but can be found in any organization [39]. At present, adequate risk management and measurement are indispensable for every organization and executives recognize that this implies the necessity of including also Operational Risk [37]. Today, Operational Risk Management (ORM) is widely used in many large corporations in the USA, Canada, Europe and Australia [16].

Where Operational Risk may arise from

Nowadays, globalization has led to the creation and use of complex products and services in every business entity. Meanwhile, the rapid development of Information Technology systems and their incorporation in organizations have led to exposure to new uprising risks different than but as significant as Credit and Market Risk [49]. Therefore, Operational Risk can appear due to a failure in one of the organization's core processes, whether this is an operating, manufacturing or processing service or capability [52].

In general, operational risk events or losses arise from:

i Processes at the points where they cross functions, business lines or business departments, in other words when a different group of people has to take control of it.

ii Interactions with external entities.

iii All types of risk can aggregate together after new systems and processes are put into practice in the organization. [16]

[15] Barings Bank was a British merchant bank founded in 1762. It collapsed in 1995 due to a manager erecting the trading operations in Singapore.

More specifically, some factors that can increase Operational Risk in an organization, as listed in [45], are among others: inadequate segregation of duties, insufficient training, lack of management supervision, inadequate auditing procedures and security measures, poor systems design and poor Human Resources politics. As far as the technology part is concerned, programming errors, errors caused by the implementation of new applications or applications that are not compatible with the already existing software and hardware are some critical factors that can contribute to Operational Risk [18].

To sum up, there are four (4) main causes of Operational Risk: people, processes, systems and external factors (Figure 1[29]). Every failure or downtime caused by or to any of these objects increases the Operational Risk of an organization.

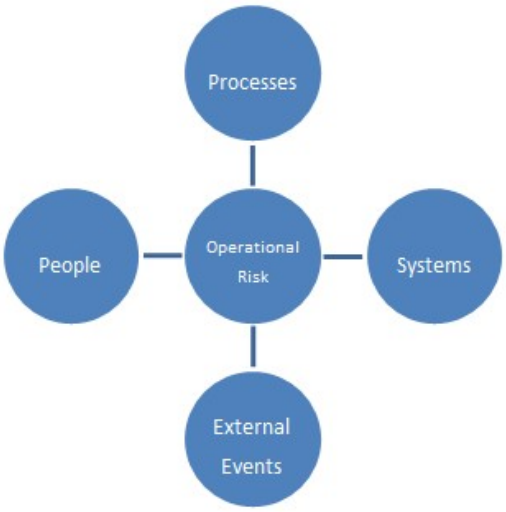


Figure 1: What Operational Risk includes (as found in [29])

Why Operational Risk has become important

Throughout the past years, financial markets have gone through a process of deregulation and thus they have become much more sophisticated and complex than before. As a result, a stronger dependence on operational activities is observed, with potentially increased Operational Risk [37]. Therefore, nowadays plenty of legislation and management frameworks of managing Operational Risk can be found, both on national and international levels [33].

Moreover, the indispensability of technology in the world of banks, and also in the business world in general, dictates the consideration of Operational Risk in every organization. This is obvious judging from the fact that nowadays IT systems are an essential part of all organizations. Moreover, considering that many of them are used or shared on a global basis, the structure behind these interconnected systems becomes much more complicated, with a highly larger possibility of operational losses arising. As Basel Committee suggests, the all-IP world where all kinds of data, multimedia and even building maintenance systems may share the same resources and technologies, makes Operational Risk worth of serious consideration [33]. In a completely digitalized environment of interconnected databases, software systems and application-converged IP networks, one technology failure may result on a high-impact

operational failure and loss ([33], [37]).

More specifically, there exist some particular examples in the literature which prove the importance of Operational Risk in the modern business world [33]:

i Ratings are related with Operational Risk, as it can be seen when S&P [16] published in November 2007 a Request for Comments (RFC) page in order to discuss their approach for managing Operational Risk parallel to Credit Risk. This was part of a thorough Enterprise Risk Management (ERM) system which was initially intended to be implemented in non-financial companies.

ii During the past years, Operational Risk has become more important for the executive managers of the companies, whereas until now they thought that it was only the employees of the lower levels that had to be concerned about this kind of risks. There are also regulatory requirements which oblige executive management members to go under Operational Risk assessments in order to successfully pass the audits that are made. One example of a regulatory requirement like that is Sarbanes Oxley, which was signed in the USA in 2002.

iii There are also service-delivery assessments that mandate the involvement of executive management in the Operational Risk Management process. For the most part of it, this is caused by the pervasive presence of the IP-protocol in every service. As mentioned in [33], large organizations assess both themselves and their main suppliers for Operational Risk, mainly linked with technology and underlined by service delivery processes. Examples of such frameworks are the SAS 70 audit in the USA and the CICA 5970 audit in Canada.

Operational Risk compared to other types of Risk

Operational Risk is tightly interconnected with other types of risk that exist in an organization, namely market, credit, liquidity and technology risk. In practice, if the operations in an organization were perfect and no failures existed, also the other types of risk would decrease by a significant amount ([33], [45]). However, no matter how interconnected the different types of riks are, they are also quite separate, mostly because of the people that are involved in each one of them. For example, mostly bankers are involved with Credit and Market Risk, whereas policemen, military personnel, bureaucrats, emergency and technology experts are responsible for Operational Risk [33].

Operational Risk for Executive Management

As mentioned before, Operational Risk has become significantly important for the board of executives of every organization, as it is crucial for the soundness of audits and financial results [33]. Operational failures are observed mainly in the lower levels of the business departments, and this is the part of the business where self-assessments, measurements and collection of event data are done. However, due to differences in the way employees in each business department perform these tasks and unwillingness to share information on these techniques, it is difficult for the top management to integrate and connect seamlessly these parts to a universal enterprise-thorough Operational Risk Management framework ([29], [33]).

Operational Risk events

The number of events that can be considered threatening or probable to evolve as operational

[16] Standard & Poor's (S&P) is an American financial services company. It belongs to McGraw Hill Financial which publishes financial research documents.

risks are in the best case several and in the worst case uncountable [31]. Some of these events include: fraud whether conducted from employees inside the company or people and organizations external to the company, violations of the professional code of conduct, excessive risk-taking, conscious or unconscious human processing errors and operating failures, IT failures (hardware or software), external attacks, accidents and natural disasters ([29], [37], [45]). In addition, as stated in [45], "sales practice violations and unauthorized trading activities" are often encountered as Operational Risk events, and in reality it is common for violators to intend to financially help their organizations but only in the short-term, without regarding the further consequences in the future.

In the effort of narrowing down the large number of different Operational Risk events, Basel Committee on Banking Supervision grouped them in seven (7) categories which can be seen in Table 5. For a further categorization, Basel II refers also to the specific Business Lines that the aforementioned events may occur (Table 6).This way, one can call upon a specific incident by mentioning the Business Line in which it occurred and also the type of the event. At this point we should note that the particular business lines groups are mainly for financial institutions, and they need to be adjusted in order for them to be used in organizations of other types.
During the past years, several Operational Risk events have taken place, mainly in the world

Basel II Event Types
Internal Fraud
External Fraud
Employment practices and workplace safety
Clients, products and business practices
Damage to physical assets
Business disruption and system failures
Execution, delivery and process management

Table 5: Event types of Operational Risk according to Basel II

Basel II Business Lines	**Basel II Event Types**
Corporate Finance	Internal Fraud
Trading & Sales	External Fraud
Retail Banking	Employment practices and workplace safety
Commercial Banking	Clients, products and business practices
Payment & Settlement	Damage to physical assets
Agency Services	Business disruption and system failures
Asset Management	Execution, delivery and process management
Retail Brokerage	

Table 6: Business lines according to Basel II

of banks. More specifically and according to [24]:

- Metallgesellschaft AG: In 1993 Metallgesellschaft AG announced that it had lost $ 1.5 billion due to incomplete oil contracts it had signed.

- Morgan Grenfell: In 1997 Deutsche Morgan Grenfell received a fine of $ 2 million because one employee was charged of diverting money, and thus the management was blamed of not being able to control the company's operations.
- NatWest: In 1997 NatWest reported a loss of $ 77 million due to mispricing interest rate options. Unauthorized actions were also revealed that were done in order to cover the errors and the losses.
- Kidder Peabody: In 1993, an employee responsible for Kidder Peabody's government securities desk handled the company's reports in order to present larger profits.
- Prudential: A $ 2 billion settlement was given to Prudential due to the accusation of the company's employees misleading clients into investing in devalued insurance packages during a period of thirteen (13) years (1982-1995).

It is important to mention that it is not rare for some Operational Risk events to last for long periods of time and thus their consequences, measurements and evaluation will take years to complete [49]. Nevertheless, efforts have been made to specify metrics that indicate threats that could reveal possible Operational Risk events. In Table 7, as found in [30], the information one can use is classified into four (4) categories and specific metrics are provided for each of them. The first type of information one can gather is "Threat-from internal" information in order to monitor the danger of employees inside the company to exploit weaknesses consciously or not. The second type, namely "Threat-from external" refers to data for events caused by third parties or nature. Type 3 includes "Threat-to internal" information about in-company assets that are vulnerable, and Type 4 is about "Threat-to external" data on how third parties' assets are prone to be attacked or fail. Type 2 and type 4 metrics are hard to obtain, but they are useful for the preventative measures and the management of risk [30].

	Table 7 as found in [30]
Class	**Sample metrics sources**
Type 1(Threat-from internal	• Number of employees sanctioned or disciplined for misconduct weekly/monthly/annually • Average number of daily teleworkers • Number of devices missing latest security patches • Number of change requests/ outages on critical assets • Number of users without current security awareness training • Number of unauthorized events observed on internal networks from internal IPs • Number of unauthorized devices observed on internal networks • Downtime due to internal equipment failures • Downtime due to administrator errors

	Table 7 as found in [30] - Continued
Type 2 (Threat-from external)	• Incidence of forest fires, earth quakes in the vicinity • Proximity to railway tracks, highways, ports and airports, industrial facilities, pipelines • metrics related to vandalism, trespassing, theft • Average number of external, uncleard visitors entering internal facilities per day • Number of unauthorized individuals/ trespassers reported weekly/monthly/annually • Logical threats to employees or assets reported weekly/monthly/annually • Which software vulnerabilities are most frequently attacked • (Apparent) country of origin of cyber/network attacks
Type 3 (Threat-to internal)	• Critical asset RTO and RPO, confidentiality and integrity assessments • Number of disaster recovery exercises in the last year • Inbound interdependency metrics (level of dependence of customers on business, level of dependence of critical infrastructures on business (energy, finance, telecommunications, safety, health, food, water, chemical and aerospace manufacturing, and government) • Number of reported infections of internal systems by viruses, worms, malware • Coverage of internal controls relative to standards (i.e. ISO 27001/17799) • Number of wireless access points • Exposure utilized in cyber attack: port, service (i.e. email, web, ftp) • Number of cyber attacks reported by firewall logs • Percentage of email blocked as "spam" by filters • Percentage of systems with anti-virus and host-based firewalls • Number of attacks on wireless access points

	Table 7 as found in [30] - Continued
Type 4 (Threat-to external	• Metrics for outbound supply-chain dependencies • Outbound interdependency metrics (level of dependence of customers on business, level of dependence of critical infrastructures on business e.g. energy, finance, telecommunications, safety, health, food, water, chemical and aerospace manufacturing, and government) • targeting metrics – what industries are being currently targeted – what type of assets are being targeted – what type of vectors are employed against selected targets – what type of vectors are most succeessfully employed – which vulnerabilities are most frequently exploited – how many compromises are undetected by internal resources (IE, bystander observations without official reporting - possibly because there is no reporting mechanism)

Table 7: Threat metrics by class

In the situation where the Operational Risk events take place, the organizations face losses, financial or not, which may include physical assets, workforce, technological assets or reputation [45]. It is not rare that some of these losses which do not affect directly the organization in monetary units, like reputation, cannot be measured accurately [49]. Moreover, it has been observed that the most harsh losses are the ones that affect the organization's core capabilities that create its competitive advantage in the market [52]. Figure 2 which was found in [45] summarizes some of the causes and the main events of Operational Risk, as well as the incurring losses.

Classification of Operational Risk

Figure 3 shows where Operational Risk is placed in relation to the total Enterprise Risk. Thus as [52] suggests, Operational Control Risk, Project Risk, Transaction Risk and Systems Risk make up Operational Risk. Moreover, this is further explained in [52] where it is indicated that Operational Risk consists of some risk subcategories such as technology risk, information risk, project risk, supply chain risk, environmental risk, management risk, occupational risk, organizational risk. In addition, in [25] counterparty risk, legal risk, business risk or business volume risk and systems or IT risk are found. Combining the existing sources, in the context of an enterprise, the aforementioned categories are presented and explained as follows ([25],[52]):

- *Technology risk*, *Systems risk* or *IT Risk* consists of events where the risk incurs from the technology realized, which is usually in the form of "business disruptions or system failures" [25]. This may include either hardware (e.g. low performance of plants or IT equipment, failed servers, damaged networks) or software (e.g. software that does not

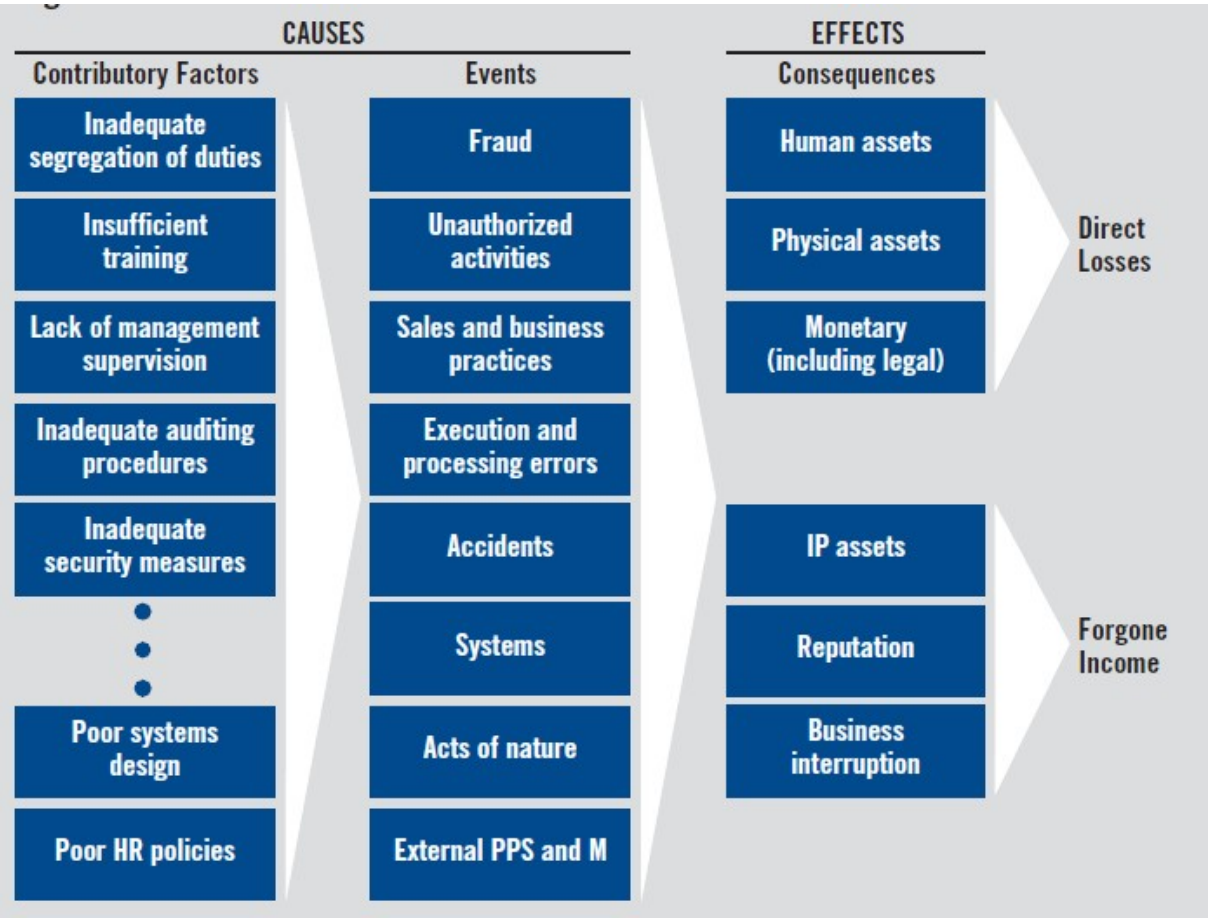


Figure 2: A generic classification scheme about causes and effects of Operational Risk (as found in [45])

fulfil its goal, software that people make inadequate use of or make many mistakes while using it [32]). It is claimed to be the most crucial subcategory of Operational Risk [25].

- *Information risk* consists of events where the risk incurs from disruptions in the required flow of information and data within the enterprise.
- *Project risk* consists of events where the risk incurs from delays and deviations on the original time and financial project limits and milestones as well as the quality objectives.
- *Supply chain risk* consists of events where the risk incurs from procurement, surveillance and delays in the logistic operations.
- *Environmental risk* consists of events where the risk incurs from the environment where the enterprise operates.
- *Business risk* or *Business volume risk* consists of events that critically modify the volume of the company's supply or demand, or the competition it faces.
- *Counterparty risk* consists of events where an organization is trading with an associate who may not be able to fulfil its obligations, endangering the performance of the first party.

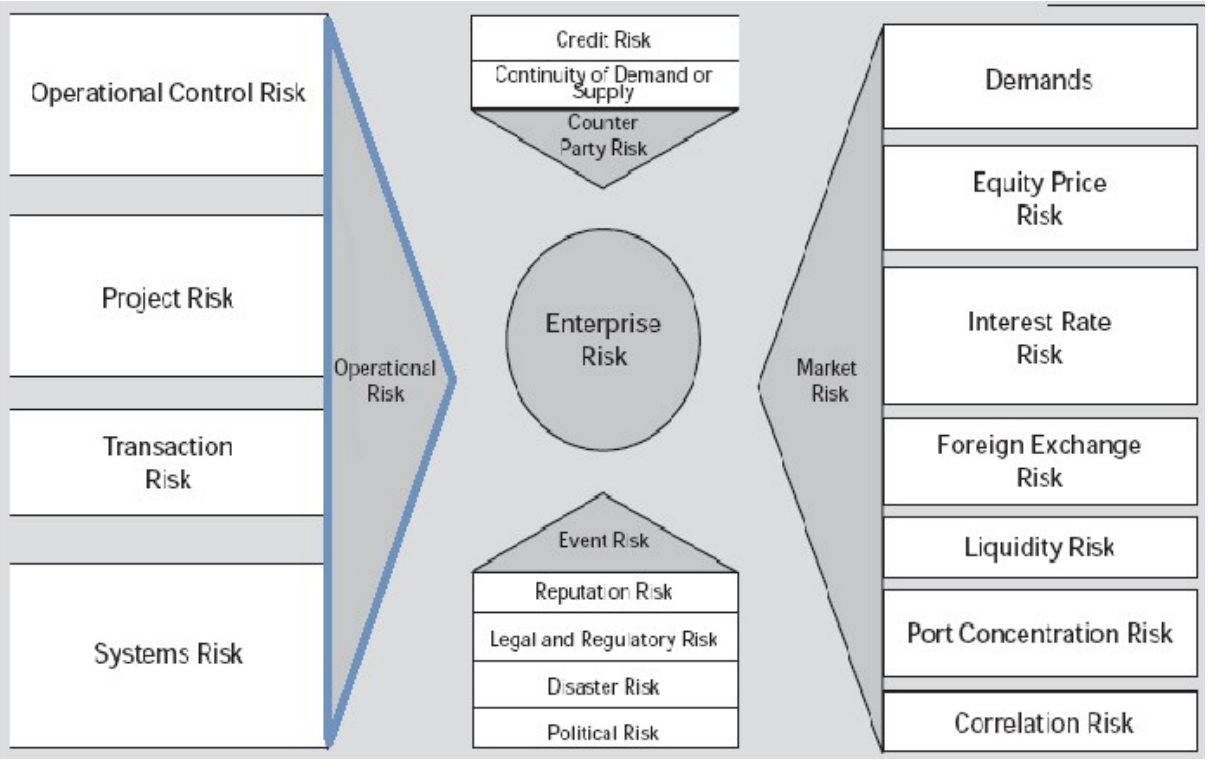


Figure 3: The position of Operational Risk in an enterprise (as found in [52])

- *Management risk* consists of events where the risk incurs from insufficient management procedures or arrangements. The more complex the organization's structure and processes, the higher the management risk will get.
- *Organizational risk* consists of events where the risk incurs from targets and objectives that are not distinctly set and assigned to people. Conflict is also included in the organizational risk sources.
- *Legal risk* which consists of events that violate the existing laws and regulations.
- *Occupational risk* consists of events that are risky for the employees' health and safety.

It has to be noted that some of the categories are included in the Operational Risk categories because they directly affect operations, such us technology or supply chain risk. However, there are others, like environmental, management and occupational risks that affect indirectly the operations, but still have impact on them and may be a cause of Operational Risk.

Similarly, a slightly different set of Operational Risk categories is found in [18]: fiduciary risk, people risk, reputational risk, technology risk and legal risk.

Operational Risk throughout an enterprise

According to Macaulay [32], human factor and IT are the most significant conductors of Operational Risk and they can be spread within an enterprise both horizontally and vertically. Horizontally, these conductors can be transferred from one business unit or department to the other, whereas vertically they can be passed on to the client or the suppliers base. In both cases, it is possible that these transportations can either accumulate and impact the receivers

(business units, suppliers, or clients) or develop from minor internal incidents to crises. However, there is also the case where human factor and IT interaction can diminish and control the effect of a crisis, especially when the monitoring system and the existing safeguards are active [32].

The interconnecting background of the aforementioned consists of the Critical Infrastructures (CIs) which as explained in [32] "are the industrial risk conductors that connect all enterprises, organizations and people into an economic ecosystem through which threats, risks, and impacts can be transmitted in an infinite number of ways". They play a significant role in the transmission of the Operational Risk conductors because they can either limit or promote it and the ongoing threats throughout the whole enterprise or towards different and unconnected organizations [32].

4.1.2 Operational Risk Management

Introduction
Operational Risk Management (also often seen as O.R.M.) consists of methods and guidelines with the goal to predict and prohibit events that may occur upon the operational procedures of a business and break or threaten their completion. It is focused on business processes and how to prevent internal or external incidents from damaging their smooth operation and consequently the fulfilment of their goals [29].

Steps of Operational Risk Management
Operational Risk Management consists of the following steps:

- Risk identification
- Risk assessment
- Risk treatment
- Risk report and monitoring

These four (4) steps make up the cycle of O.R.M.: they are executed consecutively the one after the other and constantly, that is the cycle is repeated systematically, as figure 4 shows. The ideal way to manage Operational Risk is to apply these stages both top-down and bottom-up. In the beginning, the O.R.M. cycle should be implemented at a high level (e.g. management level) in order to recognize key risks for the organization. Then, the same process should be executed from the bottom layers moving up to the top, in order to identify the risks in operations in more detail [29].

Additivity of Risk
The additivity of risk is an attribute which refers to multiple risk-generating events happening in parallel. The total incurred risk is considered to be the sum of each of the risk consequences caused by each of the events. On the other hand, we use the term non-additivity of risk in order to describe the situation when if one risk event takes place it is not likely for another one to appear at the same time, or at least not an event that will magnify the losses [31].

Figure 4: The cycle of Operational Risk Management (as found in [29])

These two opposite characteristics generate two (2) classes of Operational Risk Management approaches, depending on whether you conceive Operational Risk's nature as additive or non-additive. In the literature, the additive approach of O.R.M. can be encountered simply as additive [31] or traditional[45], whereas the non-additive approach as generic [31], integrated [31], modern [45] or all-hazards ([31], [32]).

The *additive approach* views Operational Risk as composed out of various discrete risks, each one of which requires special control treatment and security measurements. The more risks identified, the longer the list of control and security measurements gets, and as a result the more difficult and expensive to implement all of them. Moreover, since in the additive approach the risks are believed to happen simultaneously and amplify the effects of each other along with the fact that a long list of specific safeguards is too difficult to fulfil, it is a given that there will be greater Operational Risks within the organization. Lastly, this approach, which in often encountered in organizations, favours real-time control measurements and not forward-looking ones [31].

According to Macaulay [31], in the case of Operational Risk, when a risk has occurred it is not possible for another one to emerge in parallel or amplify the already incurred damage. In addition, confronting risk with separate specific tools and methods implies that the corresponding threat is expected to emerge, something that hardly never happens [31]. The traditional or additive approach provides tactical solutions for upcoming events, but fails to take into account the future layer of cause and effect and to provide techniques to manage Operational Risk from a strategic point view - like for example "optimizing the risk-control relationship in the context of the risk/loss tolerance", as mentioned in [45]. On the contrary, with an *all-hazards approach*, more generic and proactive controls are established, which is more appropriate for Operational Risk ([31], [32], [45]). It promotes forward-looking safeguards like planning, simulation, practising and building up relationships which will eventually affect business decisions ([31], [45]). Another advantage of this approach is that it provides flexibility of reaction, a characteristic which is especially valuable for events that cannot be adequately awaited [32]. These events are frequently the weak spot of many Operational Risk Management frameworks,

as "when it comes to Operational Risk, the safest bet is that we don't know what we don't know and will therefore be taken by surprise" [31].

Basel II methods for calculating Operational Risk Basel II is a regulatory requirement that is broadly used in financial institutions on a global basis [33]. Good Operational risk management means lower set-asides, better rating, cheaper capital and more willing investors.

It is believed that financial institutions that control more the Operational Risk have many benefits (for example, they can set aside less capital) that make them more competitive over other institutions. This is why in the Basel II Accord three different methods of calculating Operational Risk annual capital charge are described, so that each organization can choose the one that is more suitable for it ([33], [49]).

1. The Basic Approach
   The Basic Approach is the simplest and easiest to implement of the three methods, allocating 15% of the institution's three (3) years average gross income as a set-aside for Operational Risk ([33], [37]).

2. The Standardized Approach
   The Standardized Approach indicates that 12% to 18% of the institution's three (3) years average gross income should be granted to Operational Risk. This approach takes into account eight (8) business lines [17] in the organization's structure, and allocates a different percentage to each one of them, in the range of 12-18% [33]. The advantage of the Standardized Approach is that it is analytically tractable like the Basic Approach, but the disadvantage is that the data it requires are more detailed, complex and thus challenging to obtain [37].

3. The Advanced Measurement Approach
   The Advanced Measurement Approach, often encountered as the AMA approach, does not prescribe specific percentages or numbers that have to be saved for Operational Risk. Instead, it grants the permission to institutions to establish their own amounts according to their needs and goals, as long as they adopt and analyse explicit measurements and controls of Operational Risk ([33], [37]). There exist three (3) types of measurements in this approach, namely: scenarios, loss distribution approach and scorecard [37]. No matter what method is chosen, the AMA approach is in general the most difficult to implement, when compared to the Basic and the Standardized Approaches. This is due to the high complexity level of required data and the modelling issues which are certainly non-trivial tasks. [37]. For example, in the loss distribution approach the distribution of every operational event has to be modelled so as to simulate the overall distribution [37]. Moreover, in the scorecard method the measurements are subjective and qualitative, requiring to choose a probability measurement and subjectively set the institution's impact score [37].

However, not rarely, difficulties can be met in collecting quality data in order to calculate the Operational-Risk-related measurements. In order to define accurately these amounts, as the

[17] The eight (8) Business Lines that Basel II takes into account are, as previously mentioned: Corporate finance, Trading & Sales, Retail banking, Commercial banking, Payment & Settlement, Agency Services, Asset management and Retail brokerage

Basel II AMA approach highlights, both internal and external data as well as scenario analysis, representative of the specific circumstances (business environment and the organization's safeguards systems) are necessary [49]. Gathering valid data from these different sources can prove rather challenging. Therefore, in order to estimate the Operational Risk model a variety of techniques has been proposed in order to refine the data sets, such as: ad-hoc procedures, parametric or non-parametric Bayesian techniques and general non-probabilistic methods (e.g. Dempster-Shafer theory) [49].

Reference/Title	**Author**	**Date**	**ORM Coverage**
AS/NZS 4360: 2004, Risk Management	Standards Australia and Standards New Zealand	2004	All
AS/NZS 4801: 2001, Occupational Health and Safety Management Systems- Specification with Guidance for Use	Standards Australia and Standards New Zealand	2001	Safety Risks
CAN/CSA-Q850-97, Risk Management: Guideline for Decision Makers	Canada Standards Association	1997	All
ISO 9001: 2000, Quality Management Systems-Requirements	International Organisation for Standardisation	2000	Quality Risks
ISO 14001: 2004, Environmental Management Systems-Requirements with Guidance for Use	International Organisation for Standardisation	2004	Environmental Risks
ISO/IEC 17799: 2005, Information Technology-Security Techniques-Code of Practice for Information Security Management	International Organisation for Standardisation and International Electrotechnical Commission	2005	IT Risks
JIS Q 2001: 2001 (E), Guidelines for Development and Implementation of Risk Management system	Japanese Standards Association	2001	All

Table 8: National and international ORM standards and guidelines (as found in [2])

Tables 8 and 9 summarize the existing standards and guidelines of Operational Risk Management created by National/International and Professional institutions, respectively. Moreover, the date of their creation and what type of Operational Risk they address to are mentioned.

4.2 IT Risk

All the technological assets and different tools that are used to enable and facilitate the operations of an enterprise (such as databases, records of transactions, control and monitoring) are nowadays merged over the Internet Protocol. Although this has obviously brought up a

Reference/Title	Author	Date	ORM Coverage
A Risk Management Standard	Institute of Risk Management (IRM), Association of Insurance and Risk Managers (AIRMIC) and National Forum for Risk Management in Public Sector (ALARM), UK	2002	All
Enterprise Risk Management-Integrated Framework	The Committee of Sponsoring Organisations of the Treadway Commission (COSO), USA	2004	All
New Basel Capital Accord-Consultative Document	Basel Committee on Banking Supervision, Switzerland	2001	All

Table 9: Professional ORM standards and guidelines (as found in [2])

lot of advantages like the fact that different departments of the same company that are geographically disperse are able to access the same data and services through one shared point (e.g. an IT platform), it has also generated various imminent operational risks [17]. Except for the obvious software and hardware threats, these include all the automated processes that are taking place in computers. As all the information and communication data and services are concentrated on one location, if something goes wrong in any aspect it will spread across the different business units and affect the whole enterprise. Since there is no other alternative other than this gathering commonplace of Information and Communication Technologies (ICT), raising the preconditions and control measurements for their smooth operation in order to avoid upcoming risk seems crucial [32].

4.2.1 About IT Risk

Why IT Risk has become important

It has been stressed out in the previous chapters what an important role Information Technology (IT) plays in today's business world. Investment in IT accounts for a growing one third of the total investment budget and is the largest single investment item in US corporations. Moreover, statistics show that IT investments, without taking into account the amounts invested in software, constitute half the amount of the total budget spent on equipment [9]. Surveys have shown that IT has beneficial effects on capacity usage, inventory turnover and service or product quality [17]. As the budget amount that is allocated on IT is continuously growing, businesses exploit IT in order to create competitive advantage and achieve their strategic goals and thus business processes rely highly upon it. As a result, organizations have become extremely susceptible to IT risks, that is everything that can cause an IT error, a system interruption or a downtime, because it will affect the operation of the whole organization [9]. As it is pointed out in [20] "IT Risk always exists, whether or not it is detected or recognised by an organisation".

Why IT Risk may occur

As stated in [12], research has shown that the main causes of failures of Information Systems,

and consequently the use of IT in an organization are:

1. The fact that the people that will use the software, that is the end users, are not participating adequately in the software's development process.
2. The fact that the management does not adequately support the software - either during its development process, implementation or both.
3. The fact that the development process of the software includes too much complexity and there are high chances of risk.
4. The fact that, by implication, the introduction and implementation of a new software or system changes the environment, people's perspectives and the context within which they currently work. These sometimes thorough organizational changes face a high resistance by the people involved and the end-users.
5. The implementation process is inadequately handled.

Especially the cause of mismanagement of IT is mentioned also in [17], in which it is further elaborated that the common phenomenon of investing in IT while not actually getting the corresponding tangible benefits falls under the management's responsibility. Thus, it is pointed out that analysis and consideration of specific metrics such as ROI (Return of Investment) should be conducted, before proceeding to any investment in IT.

In [12], a survey was conducted in order to evaluate these causes and link them to Operational Risk and efficiency in enterprises. The results drove the authors to certify that the aforementioned statements are "principal causes of ICT failure" and a reason to integrate Operational Risk Management in order to tackle the imminent threats. Reversely, they conclude that avoiding these facts can lead to successful introduction, design and implementation of IT systems.

Moreover, while reviewing the literature it was found that a main cause of IT Risk is not keeping up to date with the latest technologies but using outdated systems and solutions[17]. IT Risk is likely to arise when companies focus on the past rather than looking in the future. This way, they do not grasp the best out of the latest developed innovations in order to exploit IT so as for the organization to be aligned with the continuously evolving market requirements. For example, operational risk increases due to the procedure of maintenance in old and outdated IT systems. The human resources and the time that have to be spent on it is totally proportion-less to the result. The same resources could be spent in building from the scratch or assembling new components with parts that are already on hand in order to build a new application, which would be more cost-effective and operationally safer for the enterprise [17].

A summary of the causes of IT-related risks, as extracted from [12] and [17] is presented in Table 10.

Classification of IT Risk

Although IT Risk is already a specific type of Risk, while reviewing the literature subcategories of IT risk were found in [9] and are listed as follows:

Operational Risks that connect to IT
Non-involvement of end users in the software development process
Mismanagement of IT (such as improper outsourcing or inadequate support while implementing a software)
Risks of falling behind IT
Too complicated software development processes
Project Management Risk
Quality and sophistication of software risk
Risk of slow applications development
Vendor failure risk
Human error
Resistance to change
Internal fraud through software manipulation
External fraud by intruders
Obsolescence in applications and machines
Reliability issues

Table 10: Operational Risks that connect to IT systems and their usage (as extracted from [17])

- *Sustainability risk* consists of events that may not preserve or damage the competitive advantage that IT services contribute to the enterprise.
- *Data Security risk* consists of events that involve the use of key data inside the enterprise.
- *Legal risk* which as previously mentioned consists of events that do not comply with the existing laws and regulations. In this case, these events are restricted only to the ones that do so through the usage of IT services.

Furthermore, IT Risk can evolve in three (3) domains, as proposed in [12] and [19]:

- **IT service delivery risk**, which relates to the performance and availability of IT services
- **IT solution delivery/benefit realization risk**, which relates to whether IT projects align and help the realization of business objectives
- **IT benefit realization risk**, which relates to whether IT triggers the conceptualization of new business opportunities and initiatives and whether it enhances the existing business processes' efficiency and effectiveness

Tackling IT Risk in each one of these domains, brings about corresponding results [12].
Dealing with **IT service delivery risk**:

- Enhances the smooth operation of IT services and decreases the number of disruptions in this level
- Improves the security aspect of the services
- Is more probable to ensure compliance

Dealing with **IT solution delivery/benefit realization risk** enhances:

- Project Quality

- Projects' relevance to serve the business objectives

- Projects overrun

Dealing with **IT benefit realization risk** renders IT as:

- A trigger for new business opportunities

- A facilitator of business processes' efficiency and effectiveness

IT Risk events

Risk expresses the interrelationship between the frequency with which specific events arise, and the magnitude of their effect on the organization [20]. Therefore, the IT Risk events can be categorized in two groups: the ones that occur often but have a low impact, and the ones that seldom occur but can affect or harm the enterprise significantly [25].

The first group includes events of high frequency but low impact on the organization. They cause operational losses with financial loss effects to the organizations, but fortunately these are only limited. There are really few chances that events like these will provoke the financial destruction of an enterprise. Moreover, it often happens that enterprises by default expect these losses and incorporate them in their yearly budget reports. Examples of such events can be hard drive breakdowns, disruptions of non-critical desktops or non-critical applications and deterioration of system's performance time [25].

The other group of IT Risk events contains events of low frequency but severe impact on the organization's critical components. It is obvious that these events cannot happen frequently, or it would be impossible for a typical enterprise to surpass them. Compared to the previous category, it is hard to calculate these losses and their probability to occur, in order to include them in the yearly budget reports, also because of the non-existence of enough relevant data [17]. Historical data about these events are very scarce and not precise. As a result, there exist no practical and concrete reasons to tackle these threats, as it is also possible that adopting control and mitigation techniques for them would be just a waste of money for the enterprise, as these events can also never occur during a long period of time. An example of these group of events is an overflow of a data storage device [25].

Roles of IT in an enterprise

In any enterprise, whatever its operational field or its size, on a random day, it can be observed that IT activities run through the enterprise on a regular basis. These activities are incorporated in IT processes, affecting and involving the business entity as a whole. In this context, events arise ceaselessly and they all have to be taken care of either immediately or post-hoc, depending on the severity of the event. Regardless of their severity, all these events constitute opportunities for evolving and adding value to the enterprise (not restricted to financial value/profit), but there is also risk lurking in each one of them. Risk and opportunity are strictly interconnected and tied together: in order to add business value and satisfy the stakeholders, a business should undertake particular actions that provide opportunities to achieve the goals. There is no doubt that these actions will also hide uncertainty, and thus risk within

them. As examples, decision-making about whether to employ certain technologies or software, addressing problems of existing software or Information Systems as well as building new ones and dealing with operational issues are some of the aforementioned events [20].

Finding a way to balance risk and opportunity and eventually gain benefits for the business against to the opposed threats, in other words managing IT Risk is a vital issue for every today's organization. In the context of the relationship between opportunity and risk, IT can act in various ways in an enterprise, namely as *Value Enabler*, *Value Inhibitor* or *Value Destructor*, as shown in Figure 5.

- IT as *Value enabler*
  There is a mutual serving relationship between IT and business objectives: business goals involve IT and IT serves and facilitates the business goals. New IT projects and investments aim to innovation and IT is the initiator of new business value-adding actions.

- IT as *Value inhibitor*
  This role is the opposite of the previous one. IT acts as Value Inhibitor when it fails to meet and serve the business objectives, and also fails to recognize and take advantage of new technology opportunities that could create business value.

- IT as *Value destructor*
  This role of IT occurs when specific IT events cause failures and interruptions to the operational level of the enterprise, in a range from minor to significant severity.

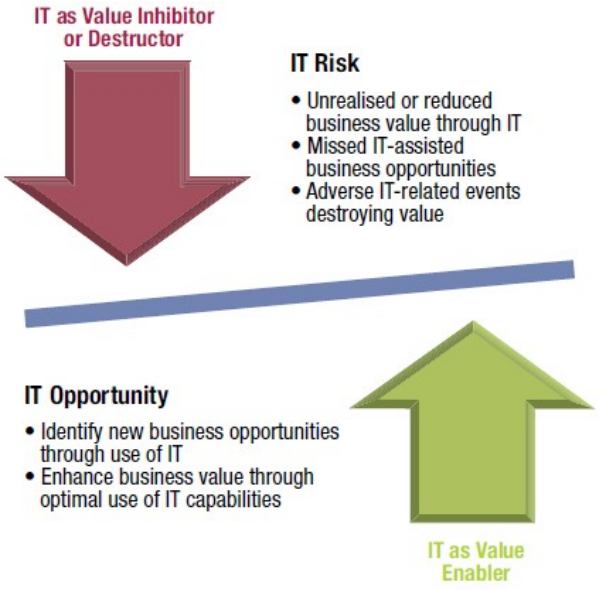


Figure 5: IT as value enabler, inhibitor or destructor (as found in [20])

On the other hand, when IT acts as a driver for the adoption, implementation and improvement of value adding activities - in other words as a Value enabler, and on top of that provides steady but also flexible IT capabilities on the operational level it can really boost the performance of the organization. This is a crucial point that needs a lot of attention: the higher the performance of an enterprise, the higher and more risks are about to come. As a result, various controls and caution measurements should be formed in order to manage and avoid

risk and its harmful results [20].

Obviously, this is hard to implement in reality. Both opportunity- and risk-looking mindset should be adopted when examining, analysing and reviewing future projects that feature IT components. In order to show how this should be done in practice, two examples, as found in [20], will be shortly discussed.

- Supposedly that a large investment in IT infrastructure has to be done, the aspects that should be taken into account are risks that may incur because of it, the advantages it will bring about, and whether it will decrease the total IT or business risk caused by other factors in the enterprise.
- When there is an emerging technology, the enterprise should examine whether it is beneficial for it to adopt it or not. Several aspects should be examined including opportunity, such as what business initiatives can be enabled by it, and also risk, such as the operating threats incurred (e.g. how to embed and support it) but also what would be the losses in case that the technology will not be adopted.

4.2.2 IT Risk Management

Introduction to IT Risk Management

IT Risk Management was first encountered in an official report in the US military and intelligence services [25]. The Defense Science Board [18] reported the document "Security Controls for Computer System" in 1970, with the goal of providing guidelines in order to "reduce the threat of compromise of classified information".

However, in the business world the concept of the necessity to manage and control risks arising in relation to IT services began some years earlier, around the 1960s, when businesses started to expand and operate in an international level. Risk Management frameworks about Software Development are found in various forms and versions, namely the basic waterfall model, or the slightly more complicated spiral and V model. These gave ground to the current concept of IT Risk Management to evolve into a process which typically includes identification, measurement, management and control of risks [25].

Difficulties in IT Risk Management

Nowadays, in the majority of the enterprises there are special departments with the responsibility to confront IT Risk Management. Even in the few ones that do not, this is inherent in the daily IT operations. Actions such as data backup and usage of more than one network providers take place in order to be prepared in case of risk events coming up [17].

IT Risk Management is not an easy procedure for an enterprise to adopt, especially nowadays that the role of a company's Chief Information Officer (CIO) is to add value to the company and not just deal with bytes [25]. Even in the organizations that do apply IT Risk Management measures, difficulties are still detected. To begin with, the absence of Risk Management

[18] The Defense Science Board is a committee of non-military experts who consult the U.S. Department of Defense on scientific, technical or other issues within the interest of the Department or the committee's members' fields of expertise.

know-how in the IT departments of the enterprise is very often. Employees usually have IT-focused competencies and do not know how to manage Risk, not to mention that sometimes they do not recognize its importance. Therefore, it is hard to express the benefits of IT Risk Management techniques in raw numbers so as to incorporate them in the enterprise's total budget and to identify the effect that they will have on the total amount of Operational Risk. Furthermore, another common problematic situation is that the measurements taken for IT Risk Management may not conform to the enterprise's business objectives. Therefore, it is advised that IT Risk Management should be incorporated in the enterprise-wide Risk Management plan and framework in order to assure that it serves the enterprise's main goals and objectives ([17], [25]).

Based on this observation, research shows that although there exist IT Risk Management approaches, many of them are rather independent, focused on specific tasks and thus not able to integrate in already existing enterprise-wide Risk Management frameworks and align to the business's objectives. More specifically, until now frameworks were found on how to tackle data security or software development processes individually, but none of them took into account whether they serve the business objectives, and this can also be considered as a factor that increases Operational Risk ([17], [25]).

Enterprise-level IT Risk Management
It was not until recently that approaches that view IT Risk Management in regards to the total enterprise risk were formulated [7]. Indicatively, some of them, as found in [7], are mentioned and their objectives are briefly described:

- ITIL - Information Technology Infrastructure Library
  ITIL's focus is on delivering best practices for Service Delivery and IT Service Management. It consists of five (5) main components, which are Service Strategy, Service Design, Service Transition, Service Operation and Continual Service Improvement [7].

- COBIT - Control Objective for Information and related Technology
  COBIT's focus is on delivering a framework for IT Governance and Control with the aim of certifying that IT is aligned with business objectives and enhances the business profitability and that IT risks are taken into account. COBIT consists of four (4) focus sub-processes , which are *Plan and Organize*, *Acquire and Implement*, *Deliver and Support* and *Monitor and Evaluate* [7].

- P3M3 - Portfolio, Programme & Project Management
  P3M3's focus is on delivering a framework for performance assessment and improvement. It helps organizations understand their Portfolio, Programme and Project Management processes and methods. It consists of five (5) maturity levels, each of which is arranged in Functional achievement/Process goals, Approach, Deployment, Review and Perception & Performance measures [7].

- ISMS - Information Security Management System
  ISMS's focus is on ensuring IT Security in all aspects. Organizations rely heavily on information, and they have to be sure that their internal data stay secure, integral, available and confidential, if necessary. Thus, according to [7], Information Security "means protection of all related assets including software, hardware, network, Internet

connectivity, application, database, data (both at rest or in transit), file and hard copy reports".

In [7], another framework for Enterprise level IT Risk Management is presented and it is claimed that there are five (5) crucial elements that support IT Risk Management in the context of an enterprise. Namely, these IT Risk Management boosters are Infrastructure Development and Support, Operations & Maintenance of Business Process Related Software & Hardware, Office Level Support, Software Development and Outsourcing Management.

Infrastructure Development and Support includes all infrastructure parts such as networks and servers as well as human resources, that is employees that are involved in their construction, design, implementation and maintenance. Furthermore, Operations & Maintenance of Business Process Related Software & Hardware includes business entities that are involved in the IT operations and services. Such entities that should be in support of IT Risk Management measurements can be project management, information security and operations, with the human factor built in all the above. In both of these support levels that include human resources and human factor respectively, it is assumed that they are sufficiently competent and able to perform their tasks.

It has to be noted that the first three (3) levels are required for the framework, whereas the rest are optional.

IT Risk Governance

Risk Governance is explained by the International Risk Governance Council[19] as "Governance refers to the actions, processes, traditions and institutions by which authority is exercised and decisions are taken and implemented. Risk governance applies the principles of good governance to the identification, assessment, management and communication of risks".

Risk Governance guidelines should be taken into account when managing IT risks in order to avoid the misalignment of IT and business objectives. As stated in [19], there are some commonly accepted guidelines about how to govern IT in an enterprise. It is advised not to isolate IT risk from the overall risks that the enterprise faces, but rather view and treat it in regards to the business strategy. Focusing on the consequences it will have on the business objectives ensures IT's role as a business enabler instead of a business inhibitor [19]. In addition, a holistic view of IT risks should be adopted, regarding the effects they will place upon the whole organization rather than just a technological scope. What is more, it is advised that the IT Risk Management measures should tackle more than one risk at a time in order to be more effective and sustainable. This can be linked to the additivity of Operational Risk as presented in Chapter 3, rendering this approach more proactive and future oriented ([19] [31], [32], [45]).

Modern IT Risk Management

Similar to Operational Risk Management, current IT Risk Management practices view it as a process consisting of four (4) stages [9]:

- Risk identification

[19]International Risk Governance Council - IRGC is an independent organization which focuses on improving the understanding and governance of systemic risks (http://www.irgc.org/).

- Risk analysis
- Risk-reducing measures
- Risk monitoring

These iterative stages can be found in the literature with slightly different names (e.g. in [25] the stages are presented as Risk identification, Risk measurement, Risk management and Risk control) or in enhanced versions with more steps, but their subject matter remains the same. As an example, in [19] a IT Risk Management framework is introduced which consists of the steps:

- Set responsibility for IT Risk Management
- Set objectives and define risk appetite and tolerance
- Identify, analyse and describe risk
- Monitor risk exposure
- Treat IT Risk
- Link with existing guidance to manage risk

In this document, the version presented in [9] will be followed as it is based in plenty of academic articles and papers. Moreover, it will be further explained in the following section, separating each stage of the process in three (3) levels: application, organizational and interorganizational level [9]. The stages are continuously repeated the one after the other like in the Operational Risk Management process, covering all the three (3) levels of the structure, as it is shown in Figure 6.

1. Risk identification
   In the *Application level*, Risk identification mainly takes place in technical features, that is where disruptions can arise in the infrastructure part or while the applications are running. These can be caused either by events occurring outside the company, by entities that are not directly linked to the company or by in-company factors. Whereas the in-company factors are mainly restricted to illegal access, fraud actions and in general improper use of systems by the company's employees (either on purpose or by accident), the external threats can vary from natural disasters to infected files and hackers' attacks.

   In the *Organizational level*, the risk events that were identified in each low-level application are put together and form the overall list of IT risks that the enterprise may face.

   In the *Interorganizational level*, a lot of the company's entities are communicating through a shared virtual environment. A typical example is multinational companies with branches that operate under a shared company name and environment, but are physically spread in locations around the world. In this kind of companies, IT plays an even more significant part, as it is the main instrument that keeps the company's smooth and consistent operation. As expected, all the risks identified in the Organizational level are aggregated and show the path that the company's high-level Risk Management should follow [9].

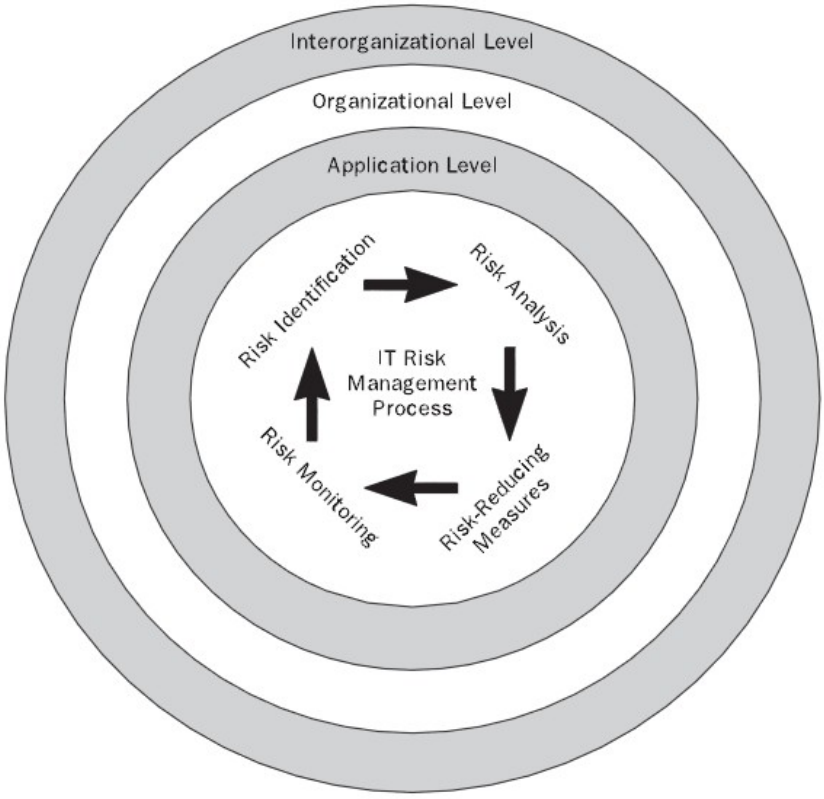


Figure 6: Three levels approach to IT Risk Management (as found in [9])

2. Risk analysis
   Similar to the Operational Risk analysis techniques, in IT Risk analysis quantitative, qualitative or hybrid methods that combine both aspects can be found. These methods should be consistently applied to all levels (*Application*, *Organizational* and *Interorganizational level*). The Annualized Loss Expectancy, the Courtney method and the Livermore risk analysis methodology are some of the available quantitative methods ([9], [41]). Scenario analysis and fuzzy metrics are examples of the qualitative methods ([9], [41]). All the aforementioned can be supported by the hybrid Delphi technique to combine results and data of both types ([9], [41]). It is not in this document's interest to further analyse these methods.

3. Risk-reducing measures
   As soon as the IT risks are identified and analysed, decisions should be taken and afterwards implemented on how to prevent these risks from actually occurring. Plenty of technologies, mechanisms and practices are on hand to use. Taking into consideration the specific requirements, strategy, budget and resources of the company along with the types of risk it is facing, the suitable method or combination of methods should be determined. Risk-reducing measures from the ones presented in Table 11 as found in [9] should be taken in the *Application*, *Organizational* and *Interorganizational level*, aiming to a complete solution for reduction and mitigation of IT Risk events.

4. Risk monitoring

Type of risk	Risk-reducing measures
Natural disasters	Disaster recovery plan (DRP)
Data security risks	Back-up files Password control Access codes Fingerprinting Palm printing Hand geometry Retinal screening Voice recognition Data encryption Call-back modems
Computer viruses	Monitoring computer usage Stringent audit procedures Employee education Use of company-provided software only Virus-scanning and virus-removing software
Strategic risks	Patent protection Innovative search for new ways to compete Formal planning and control procedures
Legal risks	Expert consultants to reduce legal risks

Table 11: Overview of risk-reducing measures (as found in [9])

In all levels individually and as a whole, the next stage is Risk monitoring. This implies that controls are made in order to evaluate whether the measures taken in the previous step were effective, that is whether the risks are now diminished. According to the result of the measures, it should be decided what further changes should be made, if necessary. This stage can be seen as an internal audit function of the Risk Management procedure, and a preparatory phase in order to recurrently commence the process.

5 Case Study

This Chapter is thoroughly dedicated to the Case Study, which is the experiment that was conducted for this thesis. In the first part it is explained why this experiment was conducted and afterwards described in detail. The second part is a presentation and analysis of the results, whereas in the last part additional observations that do not contribute to the Research Question but are worth mentioning are shown.

5.1 Experiment Motivation and Description

While reviewing the literature, it was concluded that IT systems are a common source of operational failures which add up to an organization's total amount of Operational Risk [45]. One of the main reasons for this is the fact that employees do not get sufficient training and therefore they do not have adequate knowledge of using the software ([30], [45]). This fact led us to build the Research Question: "Does employee training on a new software improve its usage so as to reduce Operational Risk?".

As already mentioned in Chapter 4, the main entities that are responsible for the appearance and alternation of Operational Risk, whether this implies its moderation or amplification, are ICT and the human factor [32]. The experiment that was conducted in the context of this thesis is meant to combine these two "Operational Risk Conductors" in order to examine what is their effect on Operational Risk. More specifically, the aspect of ICT is found in the form of a software that a hypothetical organization wants to adopt, and the Human Factor is represented by the employees of the same company that are required to use this software. This situation may lead to human errors that are going to be recorded as ICT failures, and eventually will constitute Operational Risk for the organization ([17], [32]). An obvious solution to the risk of having employees using a software of which they have inadequate knowledge, is for them to receive training by the company. As a result, this experiment was conducted to answer the Research Question and examine whether training of employees on a newly introduced software has an effect and can eventually decrease the Operational Risk of an organization.

Two groups of people used a Customer Relationship Management (CRM) software. The first group had gone through training prior to the conduction of the experiment and the second group had not. Thirty (30) people participated in the experiment, and each group was made up out of fifteen (15) users.

A document was handed in to the participants before the experiment in which the tasks they were asked to perform were given. While they were completing the tasks the screen was recorded. Afterwards, analysing one by one the recorded videos, the specific metrics described in pages 51-52 were extracted and listed.

After the completion of the required tasks, users were asked to fill in a Post-Experiment Questionnaire to acquire their basic demographic information (age, sex), their level of computer expertise, and their perception about training in general. However, the subjectivity and bias that may be inherent to the subjects' answers in the questionnaire has to be pointed out.

While reviewing the literature, no experiment was found that examined training on software in

terms of both efficiency and effectiveness. Although experiments that test training in terms of only effectiveness like in [40] or only efficiency like in [51] do exist, an experiment that analysed training on IT software and more specifically a CRM system regarding both aspects was not found in the literature. Thereupon, the fact that both efficiency and effectiveness are going to be measured in order to evaluate the groups of the users makes the experiment complete and well-justified. Therefore, the experiment will be set up in a way that it can be linked with the employees of a company that use a software and whether undergoing training can decrease the level of Operational Risk caused by failures and errors in IT systems.

Training

Training is defined as "the action of teaching a person or animal a particular skill or type of behaviour" by the Oxford Dictionary and as "the process of learning the skills you need to do a particular job or activity" by the Cambridge Dictionary. In the case of an enterprise, training is the process of preparing the employees to complete tasks that they will be given by the company in the future, usually on a regular basis. Training is carried out by specific training teams which consist of experts or people qualified in the field, ready to communicate their knowledge to the trainees. Training usually takes the form of workshops where initially the object that is going to be introduced is presented, and during the last parts the employees are required to participate in the actions they are supposed to execute. One common situation when training takes place is to prepare employees for the introduction of new software by the enterprise. With training, employees learn how to adequately handle the software, not to make mistakes and how to use it both efficiently and effectively. As stated in ISO 9241-11, effectiveness is "the extent to which the intended goals of use are achieved" and efficiency is "the resources that have to be expended to achieve the intended goals" ([15], [22]). In other words, effectiveness is about performing the task you are required to complete, whereas efficiency is about performing this task in the right way. In order to measure the effectiveness of the users, the accuracy with which they completed the tasks should be assessed. Some common metrics for this are error rates and grading the quality of the solution. On the other hand, for the efficiency of a user to be monitored, task completion time and learning time are some useful metrics that are frequently used [15].

For this experiment, training included presenting the software to the group. This means that before they performed the five (5) tasks, the way to complete them was shown to the members of the trained group by an expert. During the training, which lasted approximately four (4) minutes, the participants were free to ask questions about the tasks to the expert. Right after this, they were required to perform these tasks on their own, without any questions or guidance given by the expert any more. Their performance (in terms of efficiency and effectiveness) was measured by the following metrics:

- Efficiency
  - the time for the completion of each task
  - the total time for the completion of all the tasks
- Effectiveness
  - the number of errors that were observed during the process. In this context, each task that was not completed, or was completed in the wrong way was considered

to be an error.
(Note:in the case of let's say a word, typographic mistakes were not considered as errors.)

Test Group
Thirty (30) Bachelor, Master and Ph.D. students form the test group. Among them, the majority of the test group are Master students between twenty three (23) and twenty six (26) years old. There were almost as many male as female members, and their field of studies varied from Medical studies, to Political or Natural Sciences, with the majority of the group having a degree in Computer Science. The participants were randomly assigned to the trained or the untrained group so as for the results to be as objective as possible. In Table 12 the data are more explicitly described.

Sex		**Age**		**Academic Level**		**Field of Studies**	
Female	13	18-22	5	B.Sc. students	9	Business	2
Male	17	23-26	17	M.Sc. students	15	Computer Science/IT	13
		27-30	4	Ph.D. candidates	6	Engineering	8
		over 30	4			Natural Sciences	3
						Law	1
						Political Sciences	1
						Social Sciences	1
						Medical Sciences	1

Table 12: Sex, age, academic level and field of studies information of the Test Group

The Software
A Customer Relationship Management (CRM) software was selected as the test software of this experiment. This is due to the fact that since CRM systems are widely used in enterprises ([28], [50]), any employee, no matter his or her field of expertise may be asked in any point of his professional life to use a CRM system. Moreover, no other experiment about training on CRM software was found in the literature.

The specific CRM that was used is called "Insightly" and is a CRM targeted specifically for Small and Medium Enterprises (SMEs). It is a free, web-based software with a user-friendly interface (Figure 7), which is one of the most widely used CRM for SMEs.
The users were asked to perform five (5) tasks in the software, which are described below. Moreover, every task is marked with a Level of Complexity within a range from 1 to 3, with 1 indicating the lowest and 3 indicating the highest Complexity Level.

Task 1. Add a New Project and name it "Test Project".
The user has to find the way to create new projects in the software. Afterwards, he should fill in the given name for the project ("Test Project") in the correct fields, and save the project. There are a lot of blank fields of extra information that can be completed, such as the category of the project, who is responsible for it and in what stage it is in. The user should neglect these additional fields and leave them empty.
Level of Complexity: 2

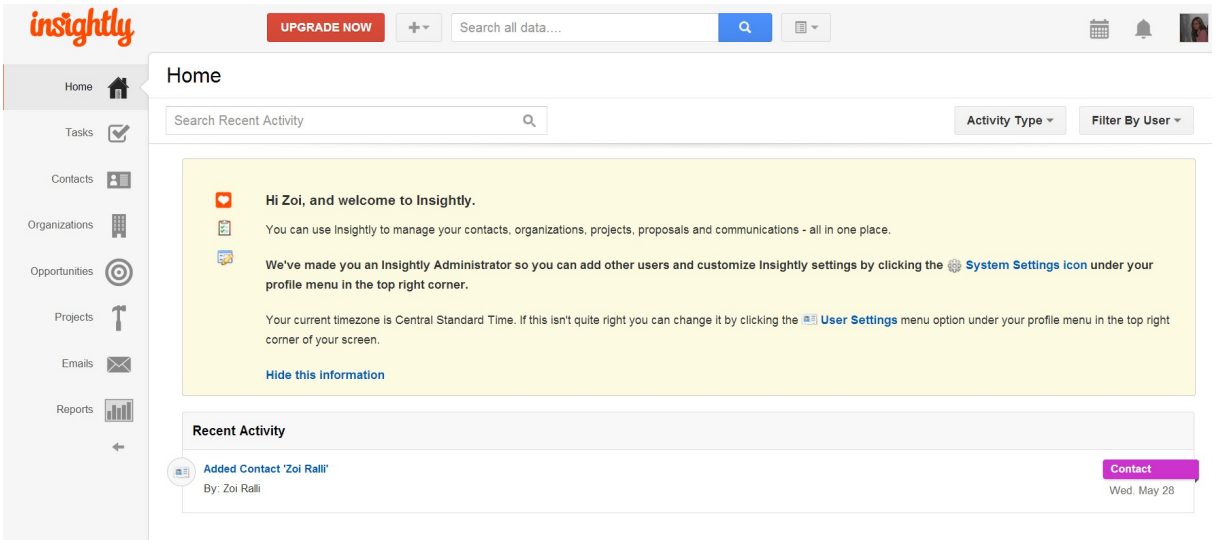


Figure 7: The homepage of "Insightly"

Task 2. Add a New Contact and name it "John Deer".
The user has to find the way to create new contacts in the software. This is similar to the previous task. Afterwards, he should fill in the given name for the contact ("John Deer") in the correct fields, and save it. There are a lot of blank fields of extra information that can be completed, such as the role of the contact, the organization he is working for and his personal email address. The user should neglect these additional fields and leave them empty.
Level of Complexity: 2

Task 3. Find the "Test Project" that you created and change its status to "in progress".
The user has to discover how he can visit again the project he created and see its details. Afterwards, he should observe that the current status of the project is described as "NOT STARTED", and change it to "IN PROGRESS" as indicated, selecting this option from a scroll down list. Again he should save the changes in the project.
Level of Complexity: 1

Task 4. Add a New Task to the "Test Project" that you created, name it "Test task" and link it to "John Deer".
The user should once more visit the project he created in Task 1. He should find the scroll down list named "Actions", and select "Add New Task For Project". After that, he should fill in the given name ("Test Task") in the correct field, leaving the rest of the fields blank. However, he should find the field named "Add New Link" and type the name of the contact he created in Task 2. As soon as he types the first letters of the contact's name, the contact will appear as an option next to the field. He should select it and save the changes before he moves on.

This is considered to be the most complicated among the five (5) tasks.
Level of Complexity: 3

Task 5. Delete the "Test Project".
The user has to find the way to delete the project he created. This is achieved by pressing a "trash bin" icon, similar to many other pieces of software. Once this is done, the user has to

confirm that he indeed would like to delete the item.
Level of Complexity: 1

5.2 Results

The mean measurements of all the metrics (time per task, total time and number of errors) were better for the group that received training prior to the experiment. The Trained group completed all the tasks in less time than the Untrained users. Consequently the time that the first group spent on all the tasks was as well less than the second group. Depending on the task, the difference of the completion time between the two groups was more significant or of small importance. Furthermore, the Trained group made on average fewer errors than the other group, and more specifically their average number of errors was 0,47 compared to the average 1 mistake that the Untrained users made. The detailed measurements for both groups with the minimum, maximum and mean completion time and the number of errors are given in Tables 13 and 14, for the Trained and the Untrained group respectively. Moreover, a graphical representation of the time that each user spent on each task for the Trained and Untrained group is demonstrated in Figures 8 and 9, respectively.

A comparison of the mean measurements for the two (2) groups is given in Table 15. A more detailed representation is given in Figure 10, where the total time that each user spent on the tasks is represented, sorted from minimum to maximum time and classified per group. Thus each line represents one group, and it is easy to compare their minimum, maximum and average time.

	Min (seconds)	Max (seconds)	Mean (seconds)
Task 1	10,28	43,12	21,65
Task 2	12,8	75,87	26,10
Task 3	15,38	37,41	21,15
Task 4	32,18	189,36	63,91
Task 5	8,51	69,08	18,01
Total time	83,93	267,05	150,81
Errors	0	2	0,47

Table 13: Minimum, maximum and average total completion time and number of errors of the *Trained* Group

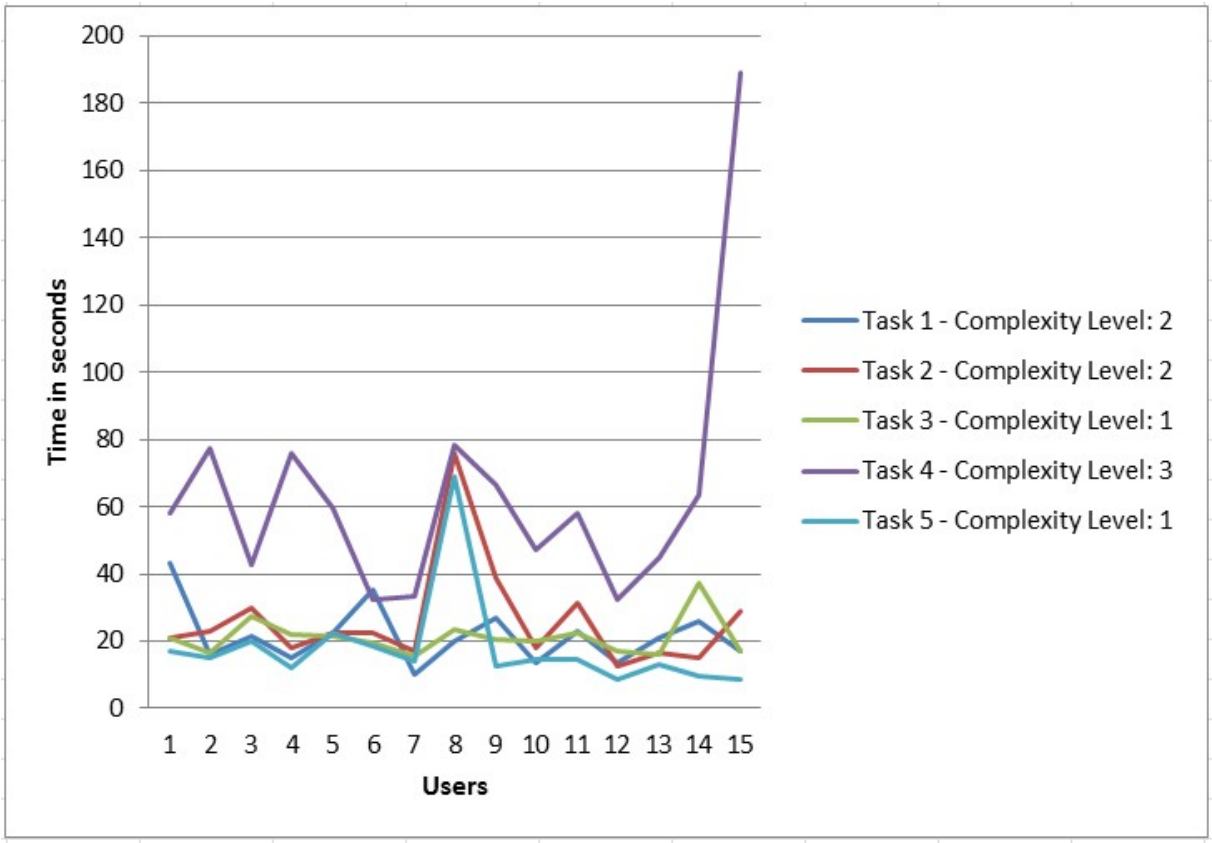


Figure 8: Time spent on each task per *Trained* user

	Min (seconds)	Max (seconds)	Mean (seconds)
Task 1	19,78	179,63	63,75
Task 2	15,93	179,98	37,12
Task 3	14,26	115,65	55,41
Task 4	31,5	249,03	98,01
Task 5	12,71	56,43	21,92
Total time	104,82	549,86	272,75
Errors	0	3	1,00

Table 14: Minimum, maximum and average total completion time and number of errors of the *Untrained* Group

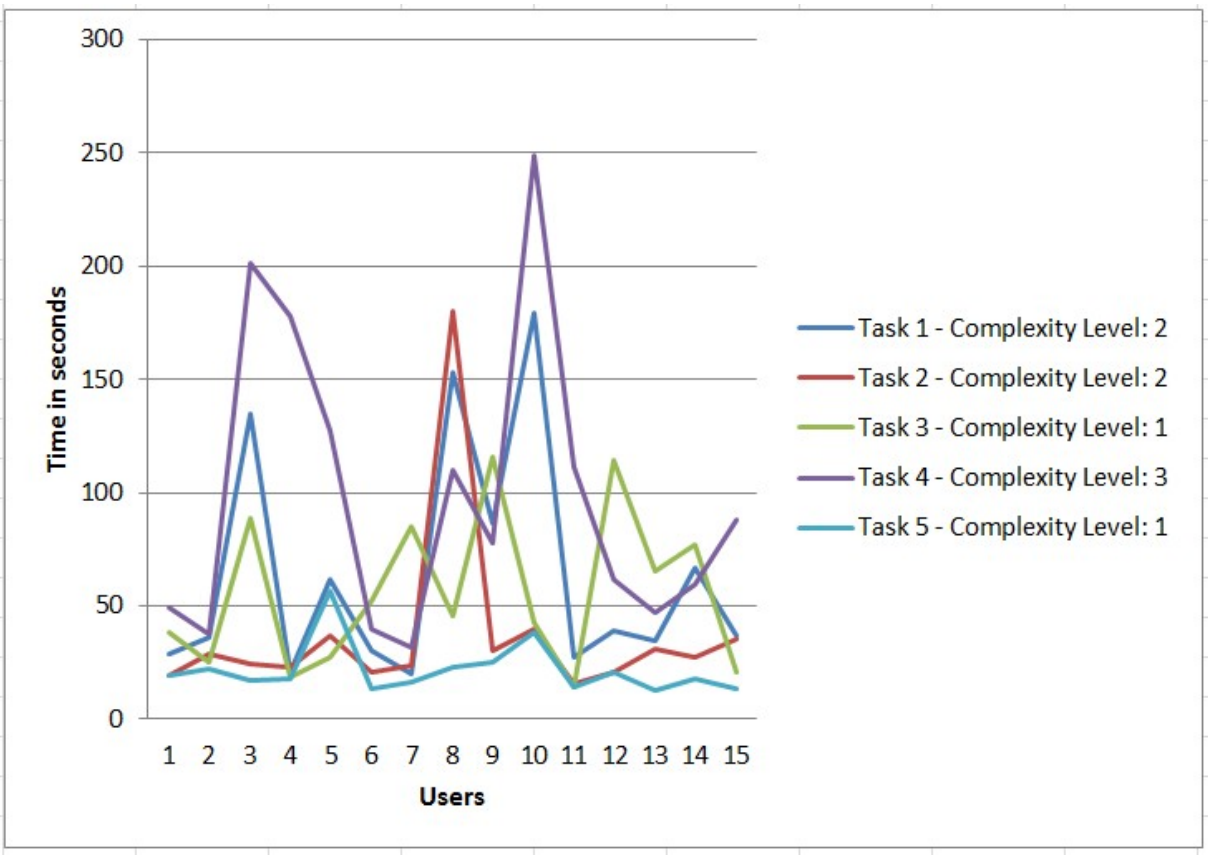


Figure 9: Time spent on each task per *Untrained* user

	Trained Average (seconds)	*Untrained* Average (seconds)
Task 1	21,65	63,75
Task 2	26,10	37,12
Task 3	21,15	55,41
Task 4	63,91	98,01
Task 5	18,01	21,92
Total time	150,81	272,75
Errors	0,47	1,00

Table 15: Comparison of the two groups' average time per task and average number of errors

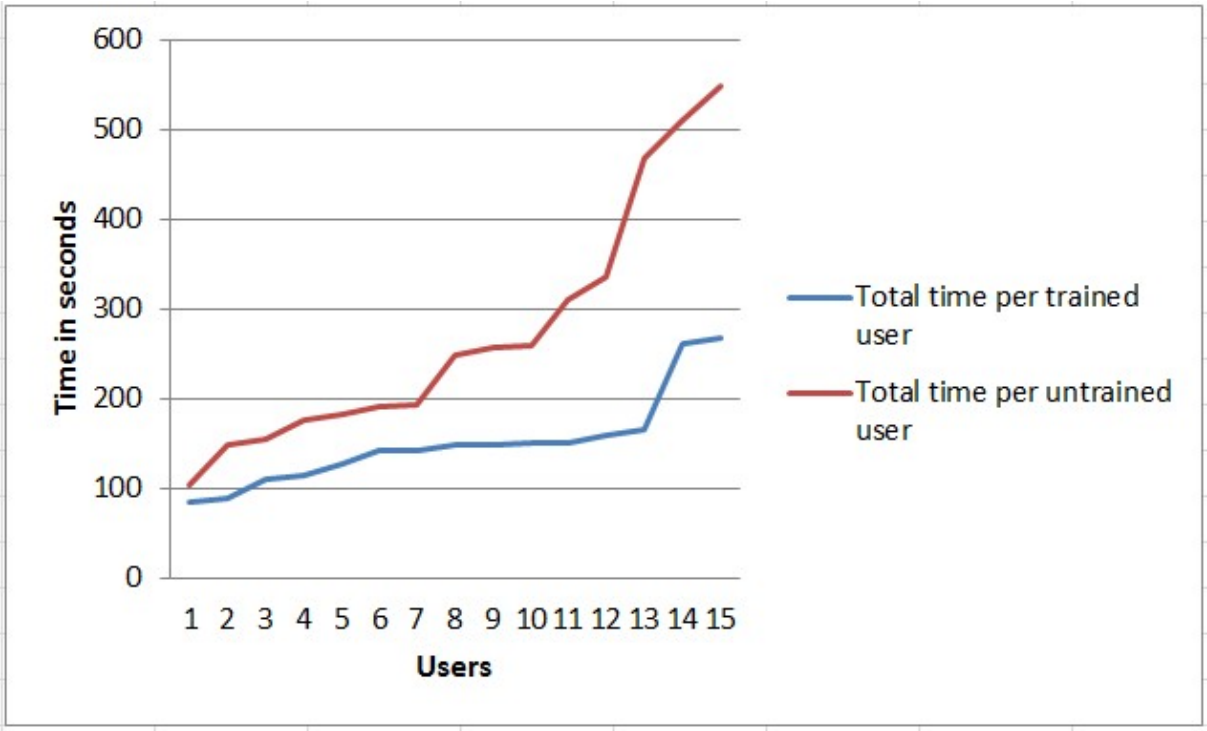


Figure 10: Total time spent per *Trained* and *Untrained* user sorted from minimum to maximum

The errors that were recorded are presented in Table 16 along with details like in which task they were made, how often they were performed both in total and per group. It can be observed that there were errors that both trained and untrained users performed. Most errors (14 out of 22) occurred in Task 4. This observation can be linked to the task's Level of Complexity, as Task 4 presented the highest Level of Complexity (3) and had the highest errors percentage. Similarly, in each of the tasks with Level of Complexity equal to 2, which are Task 1 and Task 2, 3 errors were reported in total. Finally, in the more simple Task 3 and Task 5 that are marked with Level of Complexity equal to 1, there were recorded 2 and 0 errors respectively.

Task	Type of Error	Frequency *Trained*	Frequency *Untrained*	Total Frequency
1	Created Task instead of Project	0	1	1
	User did not save the project	0	1	1
	Wrong name given to project	0	1	1
2	Last name of the contact in the wrong field	1	2	3
3	Task not completed	0	1	1
	Task not saved	0	1	1
4	Task not created in the project	3	6	9
	Task not linked to the contact	1	1	2
	Linking the project to the contact	1	0	1
	Wrong name given to the task	1	0	1
	Task added twice	0	1	1

Table 16: Types of errors, in which task they were recorded and how many times in total (Frequency), and per group (Frequency Trained, Frequency Untrained)

5.3 Secondary Observations

Task 1 and Task 2 are very similar with each other. So it was expected that the performance of the users in Task 2 would be improved, as they will get more familiar with the environment, improve with practice and gain experience on the tasks themselves ([38],[54]). However, when training is involved, the Learning Curve effect [20] may hold to a smaller extent, as training also influences the performance [1]. There is a difference between the improvements one can make through acquiring practice and experience on a task, and the levels of efficiency in tasks and processes that he can achieve by receiving training ([15], [22], [34], [38], [54]).

More specifically, it was observed that for the Untrained Group there was a significant improvement in the time they spent on completing Task 2, compared to the previous one. As it is seen in Table 15, the time that untrained users on average spent on Task 2 was 37,12 seconds, as opposed to 63,75 seconds that they devoted on average on Task 1. Moreover, the errors that they performed on average was as well decreased, from 3 to 2 (Table 16).

However, the same does not hold for the Trained group, that spent more time completing Task 2 and made on the whole more mistakes.

Female users form 43% of the Test Group, while Male users constitute the remaining 57% of it. It was observed that Female users were more efficient and more effective than the Male users. More specifically, Female users had an average total time of 186,57 seconds and an average 0,54 errors, compared to the Male's average total time of 231,06 seconds and 0,88 errors. However, the training they received has to be taken into account. Among the 13 Female users, 9 were in the Trained group with an average total time of 170,37 seconds and an average of 0,67 errors, whereas 4 were in the Untrained group with a less efficient time of 223,01 seconds but proved to be more effective, performing 0,25 errors in total. Among the 17 Male users,

[20]The Learning Curve effect has proved that the input required for the completion of a task tends to systematically decrease as the cumulative number of the produced units grows [38]

6 fell in the Trained group with an average total time of 121,47 seconds and an average of 0,17 errors in total. Both of the measurements are better than the ones of the Female Trained group. Nonetheless, compared to the Female Untrained group, the Male Untrained group was less efficient and less effective, with a total time of 290,84 seconds and 1,27 errors on average. These data are presented in Table 17. Additionally, Figures 11, 12, 13, 14 and 15 can be used in order to compare the results between the Female, Male, Trained and Untrained subgroups.

Group	**Number of members**	**Average Total Time**	**Errors**
Female *Trained*	9	170,37	0,67
Female *Untrained*	4	223,01	0,25
Female	**13**	**186,57**	**0,54**
Male *Trained*	6	121,47	0,17
Male *Untrained*	11	290,84	1,27
Male	**17**	**231,06**	**0,88**

Table 17: Female and Male subgroups, how many members they include, their average total completion time and number of errors

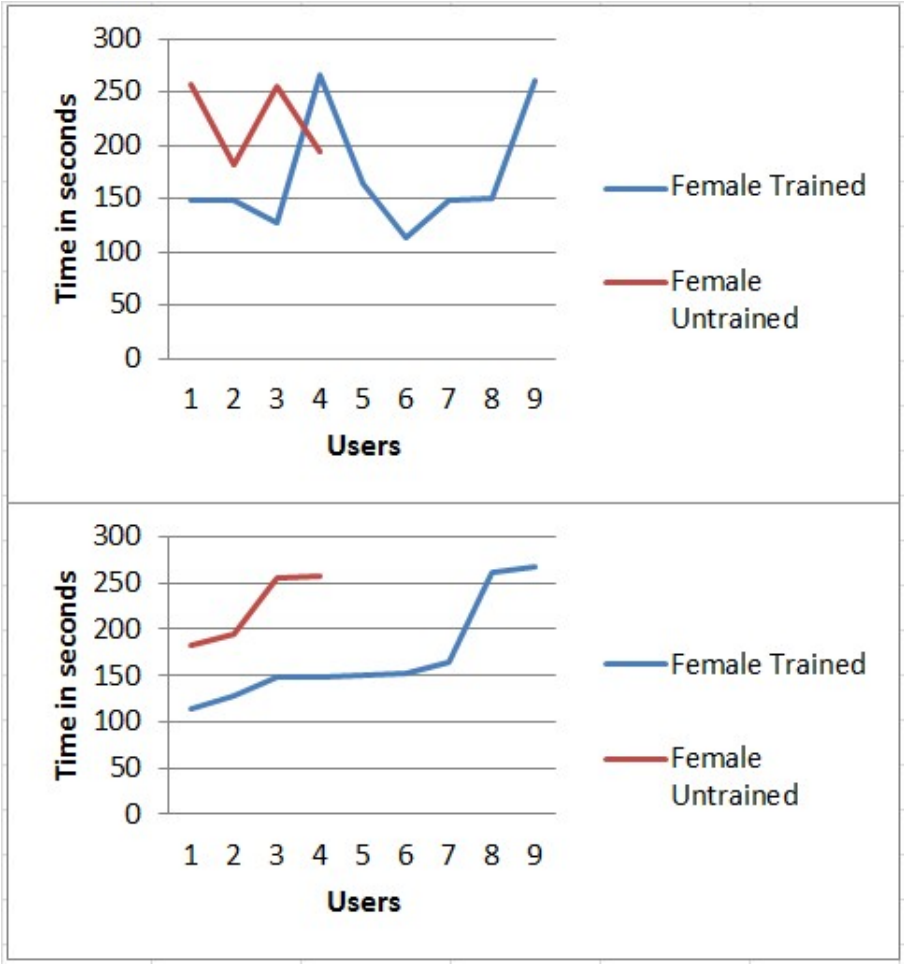


Figure 11: Total time spent per *Trained* and *Untrained* Female user, both mixed (upper graph) and sorted from minimum to maximum (lower graph)

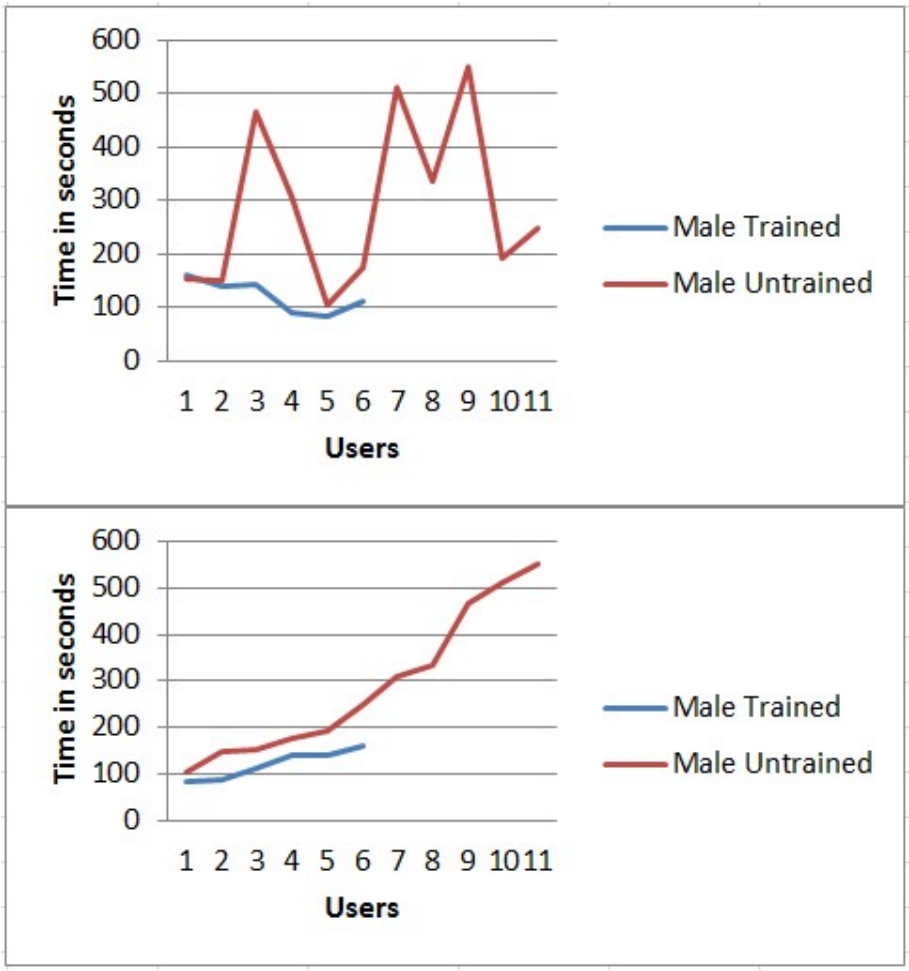


Figure 12: Total time spent per *Trained* and *Untrained* Male user, both mixed (upper graph) and sorted from minimum to maximum (lower graph)

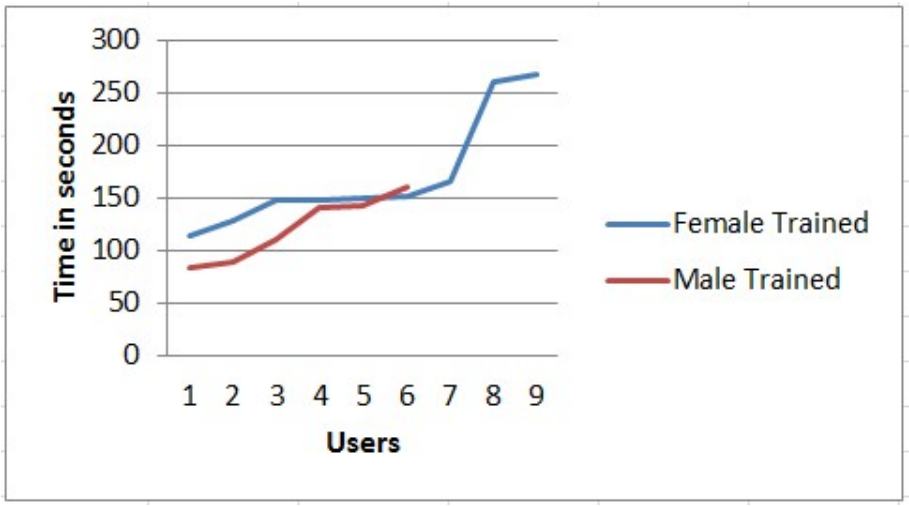


Figure 13: Total time spent per *Trained Female* and *Trained Male* user sorted from minimum to maximum

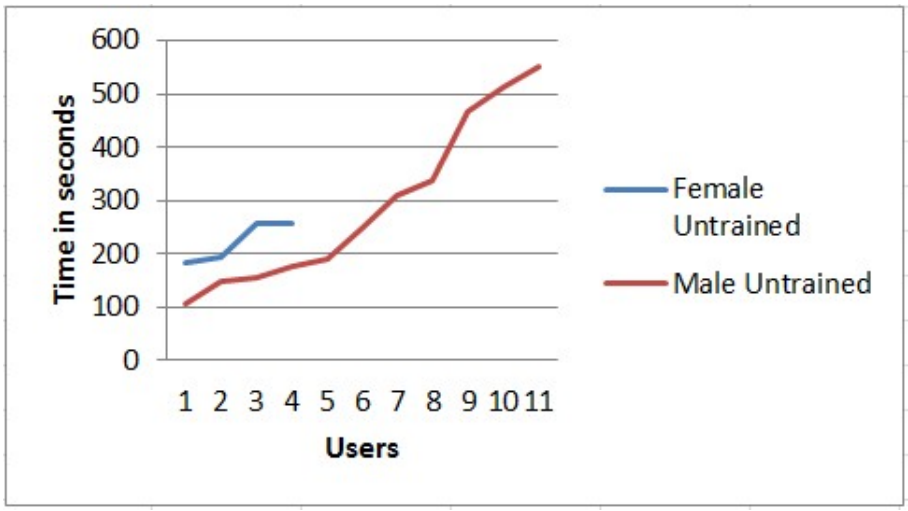


Figure 14: Total time spent per *Untrained Female* and *Untrained Male* user sorted from minimum to maximum

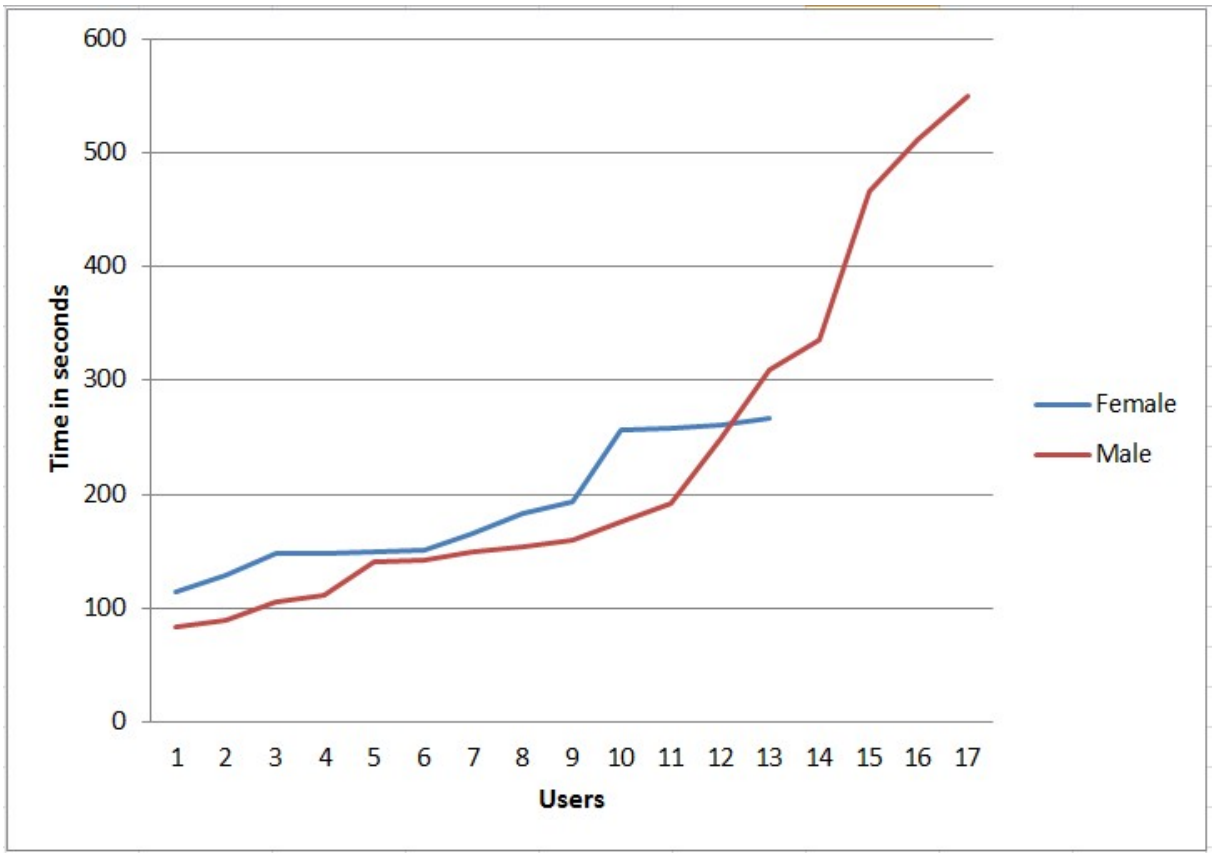


Figure 15: Total time spent per *Female* and *Male* user sorted from minimum to maximum

Among the thirty (30) users, there were fourteen (14) than made no errors. Nine (9) out of the fourteen (14) were in the Trained group, and the rest of them in the Untrained group. Moreover, the majority of them (57%) judged their level of computers knowledge as "Advanced". This subgroup had the best average total time among the fourteen users (206,15 seconds). Fewer users (29%) characterized their current level of computers expertise as Basic, and had an average total time of 207,28, which is close to the one of the previous subgroup.

Finally, none of the fourteen thinks that he has beginner's computer skills, whereas just 2 (14%) think they are experts, albeit they were less efficient than the previous two subgroups, with an average total time of 245,86 seconds.

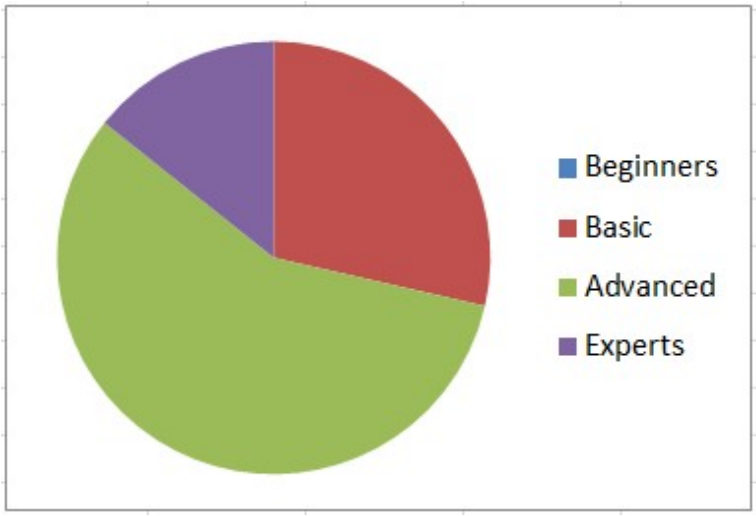


Figure 16: Level of computer skills among the users that performed zero (0) errors

The majority (73,33%) of the users that were asked claimed that they receive new software from the people that are responsible for their work (e.g. professor, supervisor, manager), which they have to learn how to use in a specific period of time. However, 60% of the test group answered that they receive training for this software only in the case where this is part of a large project or it is considered to be important for the company or their superiors. On the same question, a significant 33,33% stated that they never receive training on the software they have to use.

Furthermore, 50% of the participants added that they feel excited about the introduction of a new piece of software because it will help them finish their work more quickly and easily. Moreover, 63,33% estimates that the time they need to familiarize themselves with a newly-introduced software is less than a week.

Among the respondents that have received training on new software, the plurality found it helpful (41,67%) or somehow helpful (37,5%), whereas 78,26% prefer training as a method of learning to learning a new software by themselves.

Finally, 76,67% of the users claim to have never made a mistake that was costly for their work, due to not knowing how to use the specific software. Nevertheless, from the 23,33% that answered this question positively, 85,71% thinks that training would have helped them not to perform the aforementioned error.

6 Conclusion

By reviewing the literature, it can be concluded that IT Risk is a subsection that is included in Operational Risk. IT Risk threats are crucial for the total amount of Operational Risk of an organization, and if managed properly, part of the Operational Risk can be eliminated or lowered.

As far as the experiment is concerned, it was observed that the users that received training before using the software were both more efficient and more effective. More specifically, Trained users were more efficient in every task and consequently in the experiment as a whole, performing the tasks in 150,81 seconds on average as opposed to the average total time of the Untrained users which is equal to 272,75 seconds. Comparing these two measurements, it is derived that the difference between them amounts to 121,94 seconds, in other words approximately 2 minutes. Having in mind that all users, regardless of having received training or not, completed the tasks in 3,52 minutes, the efficiency difference between the two groups can be characterised as rather significant.

Moreover, as it was already stated, Trained users were also more effective that the Untrained users. The average Untrained user performed 1 error in the whole procedure, against the 0,47 errors than the average Trained user made. Thus Trained users made less than half of the errors that the Untrained users did, more specifically 0,53 fewer errors on average.

An important finding that should be pointed out is that in both groups, users that made errors did not realise it. They finished the experiment believing that they completed the given tasks in the right way. This is an observation that may prove dangerous for operations in an organization where its own employees may consist a threat for Operational Risk.

Through the experiment the Research Question was answered and therefore it can be concluded that *employee training on a new software can improve its usage so as to eventually reduce Operational Risk*. This holds as well for the specific software used and the tasks performed, since IT Risk is a subsection of Operational Risk and assuming that every other entity and process in an enterprise and its environment remained exactly the same for both groups, it can be claimed that training can decrease Operational Risk in an organization.

7 Discussion

In the conducted experiment, a CRM software for Small and Medium Enterprises which is called "Insightly" was used, as described in section 5.1. The software is easy to use and it is considered that any user with basic computer knowledge can fulfil the required tasks. However, it has to be noted that the language of the software used is not the mother tongue of every user, which may cause difficulties in its usage. However, this is a common situation not only in this specific experiment and software, but in general, as a lot of pieces of software (professional ones included) do not offer the choice to adjust them in one's mother tongue.

Moreover, since "Insightly" is a web-based software, the users' preference on specific Operating Systems (OS) will be of no importance. Due to this fact, although the experiment was held on Windows OS, this did not cause difficulties to users of other OS (e.g. Mac OS) as the interface and functions would be the same regardless of OS and Internet browsers. Nevertheless, since Insightly is a web-based software, and although most users conducted the experiment using the same Internet connection, the time measured can also include lags due to this.

Through the conduction of the experiment it was concluded that *employee training on a new software can improve its usage so as to eventually reduce Operational Risk*. However, specific numbers about how much training can decrease the total amount of Operational Risk in an organization could not be calculated, even for the specific software used. In order to be able to acquire specific numbers about the effect that training has on Operational Risk within an organization, an experiment that includes more tasks which are more complicated and cover every aspect of the software should be designed. Moreover, the errors that the users would make should be given a grade of significance, and according to this grade and also the number of times that they were performed, the effect that they have on Operational Risk should be more accurately extracted. Furthermore, in order to consider every possible cause that can influence the results, the correlation with the users' IT literacy should be included in this future work. In the conducted experiment, although the users were asked in the post-experiment questionnaire to judge their computer skills, their personal bias cannot be ignored. The responses to these questions are opinionated and not 100% objective, so a special IT literacy test would be suggested instead.

Finally, the conducted experiment used as measurements the users' efficiency and effectiveness, but not the users' satisfaction of the software, as this was not in the interest of the experiment. However, a recommendation for future research would be to take into account also the users' satisfaction in similar experiments, as in this way the total usability of the software, which consists of efficiency, effectiveness and usability according to ISO [22], could be indicated.

A Post-Experiment Document

Complete the following tasks in “Insightly”. Please keep in mind the order of the tasks, as given.

Tasks:

1. Add a New Project and name it “Test Project”.
2. Add a New Contact and name it “John Deer”.
3. Find the “Test Project” that you created and change its status to “in progress”.
4. Add a New Task to the “Test Project” that you created, name it “Test task” and link it to “John Deer”.
5. Delete the “Test Project”.

After you complete the tasks, you are kindly requested to fill in a PostExperiment Questionnaire.

Post-Experiment Questionnaire

Thank you for being a volunteer in our experiment, part of which is also this questionnaire. We hope that you found the experiment's environment pleasant and fun for you. The results of the experiment will be used for a master's thesis on Operational Risk in regards to Information Technology.

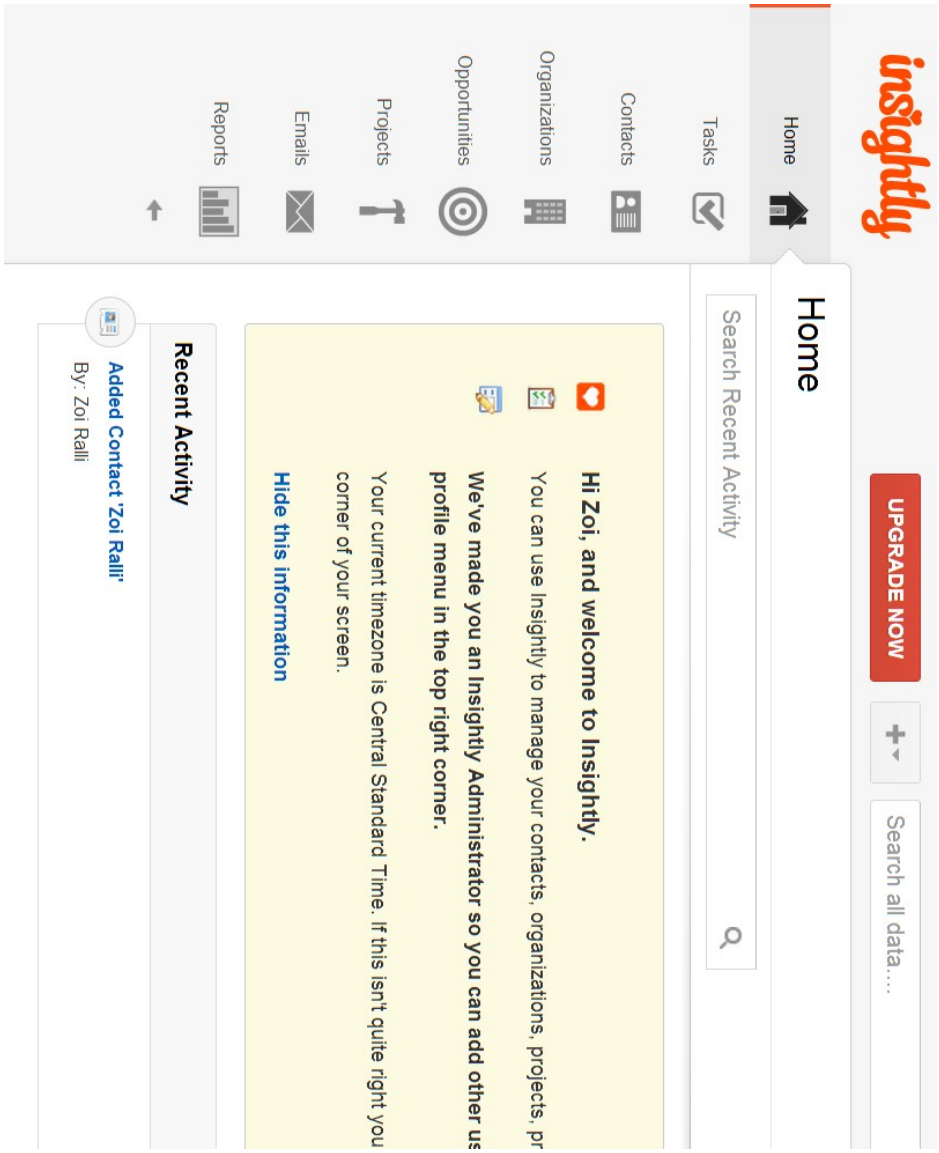
1. Sex:
   [ ] F
   [ ] M
2. Age:
   [ ] 18-22
   [ ] 23-26
   [ ] 27 -30
   [ ] over 30
3. What is your current highest academic level?
   [ ] Bachelor degree
   [ ] Master degree
   [ ] Phd candidate
   [ ] Phd
   [ ] Other. *Please specify:* _____
4. How do you judge your current level of computers expertise?
   [ ] Beginners' level
   [ ] Basic
   [ ] Advanced
   [ ] Expert
5. What is your field of studies/work?
   [ ] Finance
   [ ] Business
   [ ] Computer Science/ Information Technology
   [ ] Engineering
   [ ] Natural Sciences (Mathematics, Physics, Biology etc.)
   [ ] Law
   [ ] Political Sciences
   [ ] Social Sciences
6. Do you receive new software from the company/head of department/professor/supervisor which you are expected to master in a specific period of time?
   [ ] Yes
   [ ] No

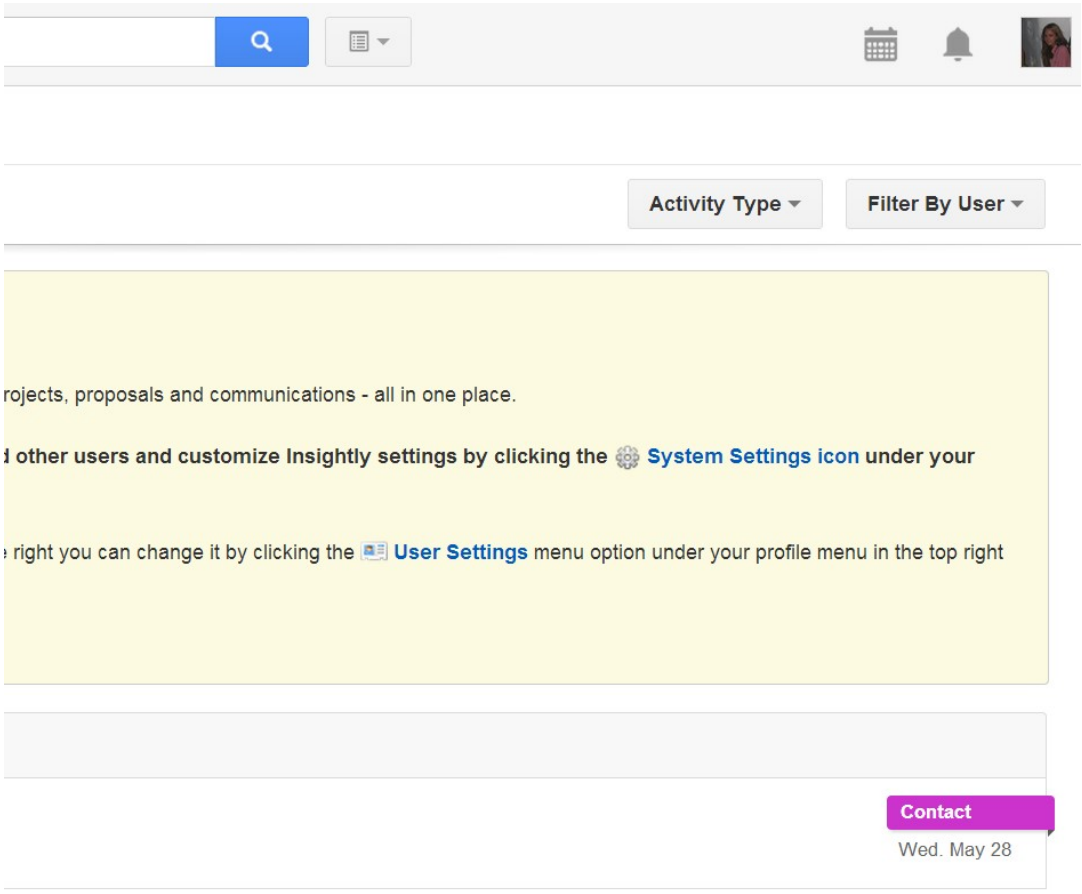
7. How much time do you need on average to get familiar with a new piece of software (provided that you use it often e.g. every day)?
   [ ] less than 1 week
   [ ] between 1 and 3 weeks
   [ ] between 3 weeks and 1,5 month
   [ ] more than 1,5 month. *Please specify:* _____
8. How do you feel when a new piece of software is introduced?
   [ ] Excited because it will help do your work more quickly and easily
   [ ] Stressed because it is time-consuming to learn how a new piece of software functions
   [ ] It makes no difference to you
9. How often do you receive training when new software is introduced to you?
   [ ] Every time
   [ ] Only for large projects/ Software that is considered to be important for the company/project
   [ ] Never
   [ ] Other. *Please specify:*_____
10. If you have received training, how helpful did you find it?
    [ ] Not at all
    [ ] Somehow helpful
    [ ] Helpful
    [ ] Very helpful
11. If you have received training, do you prefer it as a method of learning how to use new software to doing it by yourself (learning by doing)?
    [ ] Yes
    [ ] No
12. Have you ever made a mistake that was costly for your work and it was due to not knowing how to use the specific software?
    [ ] Yes
    [ ] No

If your answer in question 12 was “Yes”:

A. If yes, do you think that training for using the software would help avoid these types of mistakes?
   [ ] Yes
   [ ] No

B Insightly Interface




Activity Type
Filter By User
rojects, proposals and communications - all in one place.
d other users and customize Insightly settings by clicking the System Settings icon under your
right you can change it by clicking the User Settings menu option under your profile menu in the top right
Contact
Wed. May 28

C Experiment Results

Users	Task 1(sec)	Task 2(sec)	Task 3(sec)	Task 4(sec)	Task 5(sec)	Total time(sec)	Errors	Sex	Age	Acad. Level
1	43,12	21,21	21,16	57,82	16,83	160,14	0	B	D	B
2	16,26	23,05	16,76	77,25	15,26	148,58	1	A	B	B
3	21,63	29,76	27,23	42,65	20,08	141,35	0	B	B	A
4	14,81	17,76	22,1	75,75	12,01	142,43	1	B	A	A
5	22,21	22,56	21,48	59,32	22,63	148,2	0	A	A	B
6	35,2	22,25	19,63	32,5	18,68	128,26	0	A	C	C
7	10,28	16,95	15,38	33,18	13,91	89,7	0	B	B	A
8	20,1	75,87	23,58	78,42	69,08	267,05	0	A	B	C
9	27,01	38,88	20,25	66,43	12,8	165,37	2	A	B	C
10	13,5	18,23	20,13	47,3	14,6	113,76	1	A	A	A
11	23,18	31,13	22,61	58,27	14,68	149,87	0	A	B	A
12	13,54	12,8	16,78	32,18	8,63	83,93	0	B	C	B
13	21,01	16,76	15,86	44,57	13,05	111,25	0	B	B	B
14	25,85	15,13	37,41	63,64	9,43	151,46	2	A	C	B
15	17,01	29,09	16,83	189,36	8,51	260,8	0	A	B	B
16	28,58	19,35	38,26	48,95	19,4	154,54	1	B	D	B
17	35,75	28,93	25,23	37,4	22,12	149,43	1	B	B	B
18	134,92	24,68	88,92	201,43	17,26	467,21	2	B	B	A
19	20,88	22,96	18,28	178,22	18,2	258,54	0	A	B	B
20	61,62	36,7	27,17	127,84	56,43	309,76	1	B	B	B
21	30,25	21,01	51,95	39,95	13,61	104,82	1	B	A	A
22	19,78	23,36	85,05	31,5	16,26	175,95	1	B	A	A
23	152,72	179,98	45,77	110,04	23,15	511,66	1	B	D	C
24	86,62	29,95	115,65	78,12	25,48	335,82	3	B	B	A
25	179,63	39,8	43	249,03	38,4	549,86	2	B	D	C
26	27,6	15,93	14,26	111,05	14,24	183,08	0	A	C	C
27	39,05	20,48	114,57	61,58	20,66	256,34	1	A	B	B
28	34,88	31,31	65,23	47,33	12,71	191,46	0	B	B	B
29	67,03	27,12	77,18	59,78	17,63	248,74	1	B	B	B
30	36,93	35,31	20,63	87,97	13,24	194,08	0	A	B	B

Question 6	Question 7	Question 8	Question 9	Question 10	Question 11	Question 12	Question 13
A	B	A	B	D	A	B	
A	A	A	B	D	B	A	A
A	B	B	C			B	
B	A	C	B	C	A	A	B
A	A	B	A	C	A	B	
B	A	A	C	D	A	B	
B	A	A	C	D		B	
A	A	A	C	B	B	B	
B	A	A	C			B	
B	A	C	B	D	B	B	
A	B	C	B	B	A	B	
A	A	A	B	C	A	B	
B	B	B	B	C	A	A	A
A	A	C	B	B	A	B	
A	B	B	B	B	A	B	
A	B	B	C	C	A	B	
A	A	A	D	C	A	A	A
A	C	B	B	B	A	A	A
A	A	C	B	C	A	B	
A	A	A	B	B	A	B	
A	A	A	B	B	B	B	
A	A	A	B			A	A
A	A	A	B	C	A	B	
A	C	C	C			B	
A	B	B	B	C	A	A	A
A	A	A	C		B	B	
A	B	C	B	B	A	B	
B	A	A	C	B		B	
A	B	A	B	C	A	B	
B	A	C	C			B	

References

[1] Paul S Adler and Kim B Clark. Behind the learning curve: A sketch of the learning process. *Management Science*, 37(3):267–281, 1991.

[2] Hasan Akpolat and Thitima Pitinanondha. A framework for systematic management of operational risks. *Asian Journal on Quality*, 10(2):1–17, 2009.

[3] BJM Ale. Risk assessment practices in the netherlands. *Safety Science*, 40(1):105–126, 2002.

[4] Terje Aven. A risk concept applicable for both probabilistic and non-probabilistic perspectives. *Safety science*, 49(8):1080–1086, 2011.

[5] Terje Aven and Vidar Kristensen. Perspectives on risk: review and discussion of the basis for establishing a unified and holistic approach. *Reliability Engineering & System Safety*, 90(1):1–14, 2005.

[6] Terje Aven and Ortwin Renn. On risk defined as an event where the outcome is uncertain. *Journal of risk research*, 12(1):1–11, 2009.

[7] Nadhirah Azizi and Khairuddin Hashim. Enterprise level it risks: An assessment framework and tool. In *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on*, volume 3, pages 333–336. IEEE, 2010.

[8] Inga Skromme Baird and Howard Thomas. Toward a contingency model of strategic risk taking. *Academy of Management Review*, 10(2):230–243, 1985.

[9] Kakoli Bandyopadhyay, Peter P Mykytyn, and Kathleen Mykytyn. A framework for integrated risk management in information technology. *Management Decision*, 37(5):437–445, 1999.

[10] II Basel. International convergence of capital measurement and capital standards: a revised framework. *Bank for international settlements*, 2004.

[11] Anass Bayaga and Stephen Flowerday. A conceptual operational risk model for smes: Impact on organisational information technology. In *Information Security for South Africa (ISSA), 2010*, pages 1–8. IEEE, 2010.

[12] Anass Bayaga and Stephen Flowerday. Principal causes of information communication technology (ict) risk failure in an sme. In *Cyber Security (CyberSecurity), 2012 International Conference on*, pages 152–156. IEEE, 2012.

[13] Anass Bayaga, Stephen Flowerday, and Liezel Cilliers. Valuing information technology (it) and operational risk management.

[14] Peter L Bernstein and L Bernstein Peter. *Against the gods: The remarkable story of risk*. Wiley New York, 1996.

[15] Nigel Bevan. Quality and usability: a new framework. *Achieving software product quality, van Veenendaal, E, and McMullan, J (eds)*, 1997.

[16] Deborah Buchanan and Michael Connor. Managing process risk: Planning for the booby traps ahead. *Strategy & Leadership*, 29(3):23–28, 2001.

[17] Dimitris N Chorafas. *Operational risk control with Basel II: basic principles and capital requirements*. Butterworth-Heinemann, 2003.

[18] Muazam Rashid Dar, Muhammad Azeem, and Omar Masood. Operational risk management, risk management approaches, and risk mitigation techniques: Challenges faced by islamic financial services.

[19] Urs Fischer. Identify, govern and manage it risk part 1: Risk it based on cobit objectives and principles. *ISACA JOURNAL*, 4, 2009.

[20] Urs Fischer. Identify, govern and manage it risk part 3:techniques and uses for risk it and its supporting materials. *ISACA JOURNAL*, 6, 2009.

[21] Baruch Fischhoff, Stephen R Watson, and Chris Hope. Defining risk. *Policy Sciences*, 17(2):123–139, 1984.

[22] Erik Frøkjær, Morten Hertzum, and Kasper Hornbæk. Measuring usability: are effectiveness, efficiency, and satisfaction really correlated? In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 345–352. ACM, 2000.

[23] Ralf Gaese. *Risk Management and Risk Measurement: A Geometric Approach to Risk Space Analysis*. PhD thesis, University of St. Gallen, 1999.

[24] Charles Goodhart. Operational risk. Technical report, Financial Markets Group, 2001.

[25] Daniel J Hinz. High severity information technology risks in finance. In *System Sciences, 2005. HICSS'05. Proceedings of the 38th Annual Hawaii International Conference on*, pages 64c–64c. IEEE, 2005.

[26] ISACA. *The Risk IT Framework*. ISACA, 2009.

[27] Stanley Kaplan and B John Garrick. On the quantitative definition of risk. *Risk analysis*, 1(1):11–27, 1981.

[28] SCL Koh and S Maguire. Identifying the adoption of e-business and knowledge management within smes. *Journal of Small Business and Enterprise Development*, 11(3):338–348, 2004.

[29] Ioanna Lykourentzou, Katerina Papadaki, Apostolis Kalliakmanis, Younes Djaghloul, Thibaud Latour, Ioannis Charalabis, and Epaminondas Kapetanios. Ontology-based operational risk management. In *Commerce and Enterprise Computing (CEC), 2011 IEEE 13th Conference on*, pages 153–160. IEEE, 2011.

[30] Tyson Macaulay. Forward-looking risk metrics : Additivity of risk. *www.tysonmacaulay.com*.

[31] Tyson Macaulay. Operational continuity: Additivity of risk. *www.tysonmacau*.

[32] Tyson Macaulay. Risk conductors. *Information Systems Security*, 15(6):12–24, 2006.

[33] Tyson Macaulay. Convergence of operational and credit risks: Additivity of risk. *www.tysonmacaulay.com*, 2008.

[34] Carter McNamara. Employee training and development: reasons and benefits. *The Free Management Library*, 2007.

[35] Duncan Meldrum. Country risk and foreign direct investment. *Business Economics*, 35(1):33–40, 2000.

[36] L Meulbrook. Total strategies for company-wide risk control. *Financial Times*, 9:1–4, 2000.

[37] Sovan Mitra. Operational risk of option hedging. *Economic Modelling*, 33:194–203, 2013.

[38] David Bruce Montgomery and George S Day. *Experience curves: evidence, empirical issues and applications*. Marketing Science Institute, 1985.

[39] Imad Moosa and Larry Li. An operational risk profile: the experience of british firms. *Applied Economics*, 45(17):2491–2500, 2013.

[40] Gabriele Piccoli, Rami Ahmad, and Blake Ives. Web-based virtual learning environments: A research framework and a preliminary assessment of effectiveness in basic it skills training. *MIS quarterly*, pages 401–426, 2001.

[41] Rex Kelly Rainer Jr, Charles A Snyder, and Houston H Carr. Risk analysis for information technology. *Journal of Management Information Systems*, pages 129–147, 1991.

[42] Ortwin Renn. Concepts of risk: a classification. 1992.

[43] Eugene A Rosa. Metatheoretical foundations for post-normal risk. *Journal of risk research*, 1(1):15–44, 1998.

[44] Eugene A Rosa. The logical structure of the social amplification of risk framework (sarf): Aferatheoretical foundations and policy implications. *The social amplification of risk*, page 47, 2003.

[45] Ali Samad-Khan. Modern operational risk management. *Emphasis*, 2:26–29, 2008.

[46] S Prakash Sethi and KAN Luther. Political risk analysis and direct foreign investment: Some problems of definition and measurement. *California Management Review*, 28(2), 1986.

[47] Michael Shafer and Yildiray Yildirim. Operational risk and equity prices. *Finance Research Letters*, 10(4):157–168, 2013.

[48] Zur Shapira. *Risk taking: A managerial perspective*. Russell Sage Foundation, 1995.

[49] Pavel V Shevchenko and Gareth W Peters. Loss distribution approach for operational risk capital modelling under basel ii: Combining different data sources for risk estimation. *arXiv preprint arXiv:1306.1882*, 2013.

[50] Ilsoon Shin. Adoption of enterprise application software and firm performance. *Small Business Economics*, 26(3):241–256, 2006.

[51] Theodore M Shlechter. The relative instructional efficiency of small group computer-based training. *Journal of educational computing research*, 6(3):329–341, 1990.

[52] A Silvestri, E Cagno, and P Trucco. On the anatomy of operational risk. In *Industrial Engineering and Engineering Management, 2009. IEEM 2009. IEEE International Conference on*, pages 2174–2179. IEEE, 2009.

[53] Sim B Sitkin and Amy L Pablo. Reconceptualizing the determinants of risk behavior. *Academy of management review*, 17(1):9–38, 1992.

[54] Graig P Speelman and Kim Kirsner. Transfer of training and its effect on learning curves. *Tutorials in Quantitative Methods for Psychology*, 2(2):52–65, 2006.

[55] Charles S Tapiero. *Risk and financial management: mathematical and computational methods*. John Wiley & Sons, 2004.

[56] Xun Wang and M-A Williams. Risk, uncertainty and possible worlds. In *Privacy, security, risk and trust (passat), 2011 ieee third international conference on and 2011 ieee third international conference on social computing (socialcom)*, pages 1278–1283. IEEE, 2011.

[57] Sandra M. E. Wint. An overview of risk. RSA Risk Commission.

[58] George A Zsidisin. A grounded definition of supply risk. *Journal of Purchasing and Supply Management*, 9(5):217–224, 2003.