ECONSTOR
Make Your Publications Visible.

A Service of

ZBW Leibniz-Informationszentrum Wirtschaft
Leibniz Information Centre for Economics

Sitnikov, Catalina Soriana; Bocean, Claudiu George; Berceanu, Dorel; Pîrvu, Ramona

Article

Risk management model from the perspective of the implementing ISO 9001: 2015 standard within financial services companies

Amfiteatru Economic Journal

Provided in Cooperation with:
The Bucharest University of Economic Studies

Suggested Citation: Sitnikov, Catalina Soriana; Bocean, Claudiu George; Berceanu, Dorel; Pîrvu, Ramona (2017) : Risk management model from the perspective of the implementing ISO 9001: 2015 standard within financial services companies, Amfiteatru Economic Journal, ISSN 2247-9104, The Bucharest University of Economic Studies, Bucharest, Vol. 19, Iss. Special Issue No. 11, pp. 1017-1034

This Version is available at:
https://hdl.handle.net/10419/196408

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

https://creativecommons.org/licenses/by/4.0/

WWW.ECONSTOR.EU

Mitglied der Leibniz-Gemeinschaft

RISK MANAGEMENT MODEL FROM THE PERSPECTIVE OF IMPLEMENTING ISO 9001:2015 STANDARD WITHIN FINANCIAL SERVICES COMPANIES

Cătălina Sitnikov[1*], Claudiu George Bocean[2], Dorel Berceanu[3] and Ramona Pîrvu[4]
[1), 2), 3)] *University of Craiova, Romania*

Please cite this article as:
Sitnikov, C., Bocean, C.G. and Berceanu, D., 2017. Risk Management Model from the Perspective of the Implementing ISO 9001:2015 Standard Within Financial Services Companies. *Amfiteatru Economic*, 19(Special no. 11), pp. 1017-1034.

Article History
Received: 19 July 2017
Revised: 19 September 2017
Accepted: 13 October 2017

Abstract
In its new form, the ISO 9001:2015 standard activates and utilizes a thought pattern based on risk assessment functioning in parallel with the implementation of the system regarding quality management. Therefore, we strive to identify the risks and opportunities associated with the processes and products needed to create and implement a system of quality management based on the ISO 9001:2015 standard. This standard is defined by a strong client-based orientation, motivation and managerial involvement from the higher levels, as well as a process-based approach and a commitment towards constant improvement.
By implementing the requirements of the new version of the ISO 9001:2015 standard, the organisation needs to determine all the processes necessary to the system of quality management, as well as to identify those which include activities dealing with risks and opportunities.
Considering the importance and the impact of the requirements of the new version of the ISO 9001:2015 standard, starting from theoretical concepts and underscoring a set of research vectors, a model of financial risk assessment has been devised. The model is based on the correlation which can be established between the multiplicity of components relating to the components of the new standard structure, SL Annex, elements of an approach derived from risk patterns of processes and risk types which are assessed from the perspective of financial services companies.

Keywords: management models, ISO 9001:2015, SL Annex, ISO 31000:2009, risk-based approach, financial services companies, risk assessment

JEL Classification: G32, L1, M11, M14

[*] Corresponding author, **Cătălina Sitnikov** - inasitnikov@yahoo.com

Introduction

Risk management in financial investments entails a complex activity which is not regulated on a procedural level within an organisation. Risk-based thinking and process-based approaches introduced by the ISO 9001:2015 standard offers the opportunity of better risk management regarding financial services companies, much to the benefit of investors. In the activity of managing investment risks, the use of the ISO 31000:2009 standard is essential, as it offers the basis for the implementation of risk-based thinking as provisioned in the ISO 9001:2015 standard, as well as the framework necessary for the creation of a risk management system dealing with investments. ISO 31000:2009 was developed to provide a common approach in the field of risk management and is compatible with the new version of the ISO 9001:2015 standard.

The efficiency and the maximisation of profit are the fundamental objectives of any organisation. Regardless of size, area of activity or geographical positioning, all enterprises are constantly looking for the maximisation of profits. ISO 9001 has been created for the organisations wishing to optimise their operational excellence, gaining more and more importance as the final consumers wish to benefit from superior quality (TUV SUD, 2014).

Through the changes it has brought forth in structure as well as content, the purpose of ISO is to see ISO 9001: 2015 become the catalyst for genuine improvement, as well as enable a strategic integration of the processes dealing with goods and services within the core of the organisation's activity (NQA, 2015). Winters (2014) views ISO 9001:2015 as focusing on the creation of added value for the organisation and its clients. During the past decades, the service sector has substantially surpassed the material goods sector. ISO 9001: 2015 intends to cover all the aspects of production, including the supplies of services offered to clients.

Within the new approach provided by ISO 9001:2015, continuous improvement and the process-based approach remain in focus, but are regarded from a new perspective, that of risk management with a potential of generating opportunities or "positive uncertainties" (Bureau Veritas, 2015).

Risk management is currently a main component within any system of quality management. ISO 9001:2015 claims in its preamble the importance of "risk-based thinking" and considers that risk management must now extend to "the external supply of goods and services" and must not stop solely on basic processes. In addition, Deysher (2015) considers that ISO 9001 has included the notion of risk management implicitly from the onset of earlier versions, the 2015 version being clearer as it incorporates this concept within the framework of the system of management.

Risk-based thinking, already being a part of the process approach, means that the new version of the standard sees prevention as an integral part of processes. Although risk-based thinking views risk prevention as its main objective, through its subsequent functioning we can also identify opportunities (positive risks).

Within this context, the financial service industry is exposed to numerous risks which come from operational activities (risks regarding the market, the client and the supply chain) as well as the conditions associated with market regulations. All investments entail a certain amount of risk. In financial investment, the investors, individuals and legal entities, as well as the companies supplying financial services, from their position as intermediaries and consultants, must manage risk effectively. Risk management is a process of identifying the potential risks

of an investment and then carefully manage those risks as adequately as possible. Risk management, in the case of financial investments, is important because through this instrument risks can be reduced or enhanced based on the risk profile of the investors.

Through the introduction of risk-based thinking, the new version of ISO 9001:2015 offers the possibility of a new financial risks management model relating to companies providing financial services which will facilitate better risk management on the part of their clients, natural persons or legal entities, which will provide additional guarantees that the risks are dealt with in accordance with well established procedures. We propose a model based on the correlation which can be established between the components of the new structures of the ISO 9001:2015 standard (which can be found in the SL Annex), the ISO 31000:2009 standard, the elements of the risk-based approach of the processes and the risk profiles of the investors.

The paper is structured into six parts. After the introduction and the review of specialised associated writings, the third part presents the research methodology, based on the paper's two research hypotheses. In the fourth part, it is presented an empirical research on the policies and mechanisms of the risk-management domain inside financial and non-financial companies. The fifth part is dedicated to the construction of the integrated model of risk management. The paper ends with a series of conclusions regarding the utility of the model and the possibility for development.

1. Literature Review

The perception of risk by an individual can be affected by emotional as well as cognitive aspects, therefore risk is rarely perceived by individuals as being an objective aspect, but rather as a subjective aspect connected with the subject performing the risk analysis (Mertz, Slovich și Purchase, 1998; Ganzach, 2000; Slovic, 2000). That is why, economists specialised in behavioural finance state the fact that psychology can explain the anomalies which emerge in behavioural patterns normally characterised by a complete sense of rationality (Gilliam, Chatterjee and Grable, 2010; Marinelli and Mazzoli, 2010; Lucarelli and Brighetti, 2011). The investment risk is multidimensional, being influenced by emotional factors, by cognitive limitations and psychological characteristics (Lucarelli and Brighetti, 2011). The objective risk as measured by scientists from the field of finance is different from the risk perceived by individuals, because of the existence of elements such as preconceptions, knowledge, trust, optimism and pessimism (Gilliam, Chatterjee and Grable, 2010).

On the organisational level, the size of the investment in risk management usually depends on the frequency of risks and their impact on the activity. In the moment of adopting decisions regarding investments in complicated management procedures of organisational management risks, the costs and benefits of this investment must be compared. Stulz (2016) shows that excessive investments in risk-management can be as harmful for the organization as insufficient investments in risk-management. He considers that the management function of risks in an organisation should be independent from the general management of the organisation, having a similar mechanism with the audit function. Unlike the audit (that represents a function of checking and monitoring the compliance to certain rules), the function of monitoring and risk management can affect the profits of the organization.

A too cautious approach can lead to profits minimising and a too speculative approach can lead to significant damages and even to the bankruptcy of the company that supplies financial services.

The adequate level of independency of the risk-management function cannot be reached only through formal regulations. Landier, Sraer and Thesmar (2009) consider that formal independence cannot lead, automatically, to the independence of risk – management function within the organisation. The activity of the Chief Risk Office is, finally, evaluated by the general management of the organisation. This incomplete independence can have very different implications, in relation to the organisational culture. In a company that has speculative tendencies, this incomplete independence can be a way through which the general management of the organisation can force the Chief Risk Officer to accept risks that can lead to significant damages for the company that supplies financial services and for its clients. In a company that supplies financial services and it is dedicated to risk management in an efficient way, such an incomplete independence can lead to a collaborative climate between the risk management and the general management of the organisation fact that allows objectives' accomplishment in existing risk limits.

Risk management aims to settle and maintain the level of risk. Despite these, unexpected situations can appear, leading to significant damages, but this is not an evidence of excessive risk-taking or of mismanagement. It can be the achivement of an event with an extremly low probability, event that was considered while the organisation's strategy had been set up.

The specialty literature regarding risk management concentrated on two distinct features of rik management: on one hand - the attributes of the board of directors and its role in risk management and on the other hand the status of the Chief Risk Officer. The existence of a risk committee inside the board of directors, the frequency of meetings and their decisions, as well as the proportion of members with experience in risks' management, in this committee; these are problems that have aroused interest in the specialty literature (Stulz, 2016). Lingel and Sheedy (2012) have built an instrument that can quantify the quality of the members from the risk management committee taking into consideration the proportion of the members with experience in risk management from this committe and the frequency of meetings.

Researches made on a group of sixty banks, which were quoted on the Stock Exchange 2004-2010, led to the conclusion that a better surveillance of the risk at the board of directors' level is associated to taking a lower risk level in the proceeding year. Moreover, according to Lingel and Sheedy (2012), the Chief Risk Officer status influences an assumed level of risk. A higher status of the Chief Risk Officer leads to a smaller risk. Nevertheless, Lingel and Sheedy (2012) show that the banks that had a better risk management according to the proposed instrument, did not act better, during the crisis, in comparision to those banks that have neglected the risk management.

Therefore, an adequate risk management implies not only formal structures and experimented specialists, but also the existence of clear procedures that are recognisable and assumed by the entire organisation.

Other studies explore the relationship between risk and other variables that are tied to the status of the Chief Risk Officer. Kashyap (2010) and Keys et. Al. (2009) study the relationship between the Chief Risk Officer's salary calculated in relation to the salary of the Chief Executive Officer and the performances of the organisations during the crisis, showing that a good reward for the Chief Risk Officer led to better performances. Also, Aebi, Sabato and Schmid (2012) showed that the financial organisation in which the Chief Risk Officer presented the raports directly to the board of directors and not to the Chief Executive Officer; the raports had a better behaviour during the crisis. Ellul and Yerramilli (2013) have compiled

an index of government risk and based on the obtained results, they showed that the financial organisations which have registered higher values had better yields during the crisis. Berg (2014) shows that it is advisable for the business line to establish bold objectives, but the risk committee to monitor and to have the possibility to censor decisions. In this way, it is reached the maximization objective of profits in terms of a low risk level.

The need to create a risk management model in the sector of financial services is determined by intern and extern pressures. Some of the externe pressures are common for all companies and refer to the reforms from the corporate governamental domain in the stock exchange framework, audit institutions, institutional investors and the authorities of goverrnmental regulators worldwide. Other extern pressures are specific to the financial services sector and they come from regulators and legislators who want to be sure that the investors as well as the overall financial system are protected from unjustified risks (Miccolis, 2000).

In the opinión of OCC and Fed (2012), the term of "model" refers to "a quantitative method, system or an approach that applies statistical, economical, financial or mathematical theories, techniques and hypothesis for processing entry data in orer to obtain a series of estimates regarding future events and circumstances". According to the definition there are three main components of a model: entries represented by data and hypothesis, procedures and methods used in processing obtained data and information (including the way of reporting and using this information in the organisation's activity).

The investment models are simplified representations of reality, this simplification is inevitable, taking into consideration the complexity of the relationship between variables (Management Solutions, 2014). This simplification, a source of additional risks that have to be identified, analysed and managed as any other risk from a company.

Regulators as OCC and Fed (2012) encourage the companies to create risk management models, to establish procedures for applying the model and to define the role of risk management in the governance of the organization.

For the managers of companies that supply financial services an efficient risk management model can help them in the process of taking decisions allowing to take in consideration all types of risks (incidental risks, operational risks and financial risks). Therefore, using ISO 9001:2015 standard to create the skeleton on which to build an efficient model of risk management can generate clear procedures that allow the identification, complete understanding and taking the necessary measures to prevent and combat risks.

The ISO 9001:2015 standard introduces a holistic vision which entails the integration of technology in the core processes of production, as well as in the support processes, ensuring a flexibility in the management of quality control documents. This characteristic will provide an organisation with the possibility to certify a multiplicity of standards at the same time, the option of choosing standards being established based on the activity sector (Winters, 2014). According to Hutchins (2014), in comparison with the previous version, the context of the organisation is taken into consideration including a more comprehensive approach of the methodology of constructing the system of quality management.

Tseros (2015) believes that the most important advantages offered by ISO 9001:2015 are the securing of compatibilities with other standards, the reduction of conflicts and redundancies between the standards of a management system, as well as the minimisation of necessary paperwork.

Hunt (2014) states that the revised standard will focus on the implementation of requirements rather than the exceptions from these requirements. There are no defined limits apart from those that may render clauses inapplicable. Justifications will only be necessary to illustrate the fact that the limited application of a provision does not affect the organisation's capacity to ensure the existence of goods and services.

Regarding the ISO 9001:2015 standard, not all the processes of the quality management system contain the same amount of risks which affect the capacity of an organisation to fulfil its objectives (ISO, 2015). In the case of some organisations, the consequences of producing goods and services which are not in accordance with standards can determine only non-essential inconveniences for the client. In the case of other organisations, the consequences can be far greater and have a far-reaching impact. In this context, "risk-based thinking" offers the possibility of choosing the degree of planning and control of the quality management system.

In ISO 9000:2015, risk is defined as being an effect of uncertainty, "a deviation from what is expected", with a potential of being either positive or negative, "the uncertainty effect". The term "uncertainty" is defined as being a lack of information or knowledge regarding an event, which can be expressed in terms of impact gravity and emergence probability (Kymal and Reid, 2015). ISO 9000:2015 emphasises that risk is connected to potential events and that it is expressed through a probability of emergence and through the impact of such an event.

BSI (2015a) considers that ISO 9001:2015 not only deals with the management of risks but also compels organisations to identify opportunities, meaning positive risks. Whoever implements the standard must perform an analysis which concludes if a problem can be transformed into an opportunity. It is the opinion of BSI (2015a) that this aspect is yet another quality of ISO 9001:2015 helping organisations grow and develop by identifying opportunities and adopting an approach based on risks. The 2015 version of the ISO 9001 standard is a process-based approach. This approach will have to provide the control instruments necessary to make sure that the risks are kept down at an acceptable level, which will lead to the fulfilment of the general objectives associated with the management system. BSI (2015a) believes that the process-based approach will allow ISO 9001:2015 to generate consistent and respectable results for the organisation and enable the achievement of a sustainable development rhythm.

Taking into consideration the risk factor as it impacts the entire organisational system during the entire process ensemble, the probability to reach the intended goals is enhanced and the clients will benefit from the goods or the services they expect without any further complications (ISO, 2015). Risk-based thinking improves management, implements a proactive culture of development, increases customer confidence and satisfaction, continually strengthens the probability of reaching the aimed objectives, and reduces the probability of negative results.

The ISO 31000standard, published in 2009, explores the orientations and procedures relevant to the development of a risk management system by estimating risks, applying protocols of evasion, thus minimising the risks of such events (ISO, 2009). All of the activities of an organisation imply the identification and analysis of risks and their subsequent evaluation via the mediation of the chosen risk profile. During this process, the organisation communicates and consults with the relevant parties, constantly monitoring and revising the risks.

Nowak and Wójtowicz (2015) believe that every organisation, public or private, or any natural person can become a potential user of the ISO 31000 standard. The ISO 31000 standard constitutes the foundation of a system of management that will provide the possibility of a risk management system, the implementation of the stages of that respective system while monitoring and continually enhancing it. Establishing a risk management framework integrated in the organisational strategy and operational activity of the organisation will lead to more efficient management and the improvement of the global management system. In the opinion of Jodkowski (2015), the introduction of ISO 31000 can lead to the increase of success rates linked to the fulfilment of objectives by improving risk assessment activities as well as securing a holistic approach of the risk management system.

2. Research Methodology

This study performs an exploratory research on risk management in companies and of the way risk-based thinking can be integrated within the activities regarding risk management undertaken by the companies which provide financial services on behalf of investor clients. We have analysed the standard characteristics, procedures and clauses that are then integrated into a unitary and harmonious structure providing guarantees regarding the way of engaging risks based on the investor risk profiles. Based on this foundation, using and adapting Saunders' deductive approach (Saunders and al, 2009), a set has been constructed based on two research hypotheses which have been the lynchpin of the risk management model.

The first hypothesis of the research starts from the the exploratory research that is made in the risk management domain inside the companies and it is formulated like this:

H1: Nowadays, risk management represents an adequated, implemented and efficient function inside companies. The validation or invalidation of this hypothisis is going to be achieved after an empirical research that is going to be made on risk management inside companies and that will indicate the need of some clear procedures in this domain.

The second hypothesis of the research that has represented the initial point in creating the model has been represented by:

H2: There are differences regarding the risk management between corporations and companies that supply financial services. Starting from the specialty literature study we will research the validation of this hypothisis.

Because of hypothesis research, the risk management model will be generated starting from the integration of structures of the new standard ISO 9001: 2015 (Anexa SL) and of ISO 31000:2009 standard. The new obtained generic system of the quality management will be based on orientative thinking towards the risk and its specific elements, offering companies a set of clear procedures and mechanisms to ensure an efficient management of risks.

3. Analysis of the implementation model for risk management

Taking into consideration the present economical context that is characterized by a growth of economical uncertainty, the company's risk management became an important activity. Over time, it has been proven that taken measures were not always efficient; there are not models of risk management that can be totally accepted and that can be effective in the

majority of cases in which they were used. Taking into consideration the specific risks (systematic and non-systematic risks, fraud risks, etc) the financial sector has been a leader in developing risk management practices. Systematic failures determined by economical cycles inside the financial sector, determine a skepticism about the idea of using practices developed in this sector as a model for others (Pergler, 2012). In addition, the risk management practices in the financial sector are largely generated in response to changes in regulations imposed by different bodies regulating the market and not necessarily by uncontrolled situations occurring within the sector.

The risks that corporations are facing, in general are both financial and non-financial. Within companies providing financial services, the focus naturally falls on financial risks (eg, credit, liquidity or market), operational risk is becoming increasingly important in management decisions. In the case of non- financial corporations, the same risks exist, but the impact is not the same as for companies providing financial services. There are also risks that have a greater impact on non-financial corporations than for companies providing financial services (environmental, safety and health occupational hazards, risks of outsourcing).

Within all responible corporations for risk management there are boards of directors, but there are no universally accepted models, clear procedures on how risk management operates. Addressing the risks must be carried out in an individual way and not aggregated; risk tolerance is established for each identified risk in an individual way. Another aspect that should be considered by the boards of directors refers to the interaction of various risks that can lead to the augmentation of risk impact (OECD, 2014).

In many financial services companies and some financial corporations were hired risk managers (Chief Risk Officer) thus separating risk management function from the profit centers. Such separation is successful based on the way risks are handled within the organizational culture. The companies' evolution in which there is a risk manager during the financial crisis showed that these Chief Risk Officers were not actually able to limit excessive risk taking (Taleb, 2005). Financial crises have shown the need for restructuring and modernization of the risk function, giving greater independence to the risk function. Clear procedures need to be adapted to both large companies and small ones, both financial companies and the non-financial ones, procedures that can be integrated into the general management of the company. According to FSB, the risk management system must be a part of the whole risk management framework (FSB, 2013).

In an OECD study (2014) it is shown that, typically, the risk management function is localized in the Board of Directors and in the Audit Committee. EU Directive 2006/43 / EC on statutory audits of annual accounts and of consolidated accounts require audit committees in addition to monitoring the effectiveness of internal control and the intern audit of the company, and monitoring of risk management systems. However, according to the study OECD (2014) only four countries (New Zealand, Australia, Switzerland, Greece) record a rate of over 20% of companies that have committees within the Board of directors with explicit reference to risk management.

Starting from the researches made in the study OECD (2014) we made a census of the number of countrie (Table no. 1) which include references to the risks in responsabilities of boards of directors, audit committes, committees of risk, internal control systems or those set in the position of Risk Manager (Chief risk officer).

Table no. 1: OECD countries with demands or recommendations on risk management domain for companies listed on the Stock Exchange

	Board of Directors responsabilities	Committes at the board of directors' level		Management systems of intern control / risk	Risk managers
		Audit	Risk		
Laws	11	12	1	8	1
Regulations	2	3	1	2	0
Codes	12	12	3	13	3
OECD countries	42	42	42	42	42

Source: Based on data taken from OECD (2014)

Following the analysis, the hypothesis H1 is invalidated, at least partly because risk management requires further efforts to become an adequate and efficient function implemented inside companies. Few countries have managed to introduce laws, codes and regulations in the domain.

Researching hypothesis H2, after studying the specialty literature we found that there are some differences regarding the organization way of risk management and its role in the overall governance among corporations and companies providing financial services. Far fewer corporations (only the large and innovative ones) have a risk management manager (Chief Risk Officer) or a risk committee within the board of directors. Most corporations place risk management function within the audit committee.

In a study conducted under the aegis of McKinsey, Pergler shows that there are differences in perception between corporations and financial service companies of different areas of risk management (Pergler, 2012). While corporations are in an earlier stage in the implementation procedures and practices of risk management, companies providing financial services have developed a variety of practices thar should be strengthened through procedures and supported by software specialized in this field. The recent financial crisis highlighted financial institutions focusing on impact assessment of aggregate risk and likelihood of risks appearance. The same should happen with all corporations to adopt the best decisions.

About risk management in the financial market in the European Union it was adopted a Directive 2006/73/EC of 10 August 2006 that requires companies providing financial services to "establish, implement and maintain an adequate policy for management risk, to adopt procedures and effective mechanisms for risk management on the activities, processes and systems of the company" (European Commission, 2006). Another recommendation made to companies providing financial services refers to fixing the level of tolerated risk of the company. Depending on the nature, scale and complexity of Member States may ask to establish separate sections dealing with risk management (implementation of policies and procedures, providing reports and management consulting, ongoing monitoring of risks). Although these legislative measures were introduced in 2007, the financial crisis of 2008-2010 could not be avoided because legal norms could not be translated effectively into practice. Although today there are many risk management models, they are difficult to enforce and often do not give the expected results. It is necessary to lay the foundations for a model that can be learned and understood by people in management companies providing financial services.

Because of the research on H2 hypothesis we found that there are both similarities and differences in terms of risk management among corporations and companies providing

financial services. These differences are caused by the nature of the risks, how these risks are reflected in the organizational culture and how the company creates value added. Therefore, in our opinion we consider it necessary to have an approach of risks based on procedures that should be applicable to all corporations, but to differentiate in terms of the used tools and the specific application areas.

4. Results and Discussions

A model of risk management must provide four main aspects: objectives and areas of use, inventory of used procedures and how to relate to these procedures, inventory of potential risks as well as the documentation resulting from the procedures and that enables to operate on the model (Management Solusions 2014).

Based on results of research of the proposed hypotheses and bearing in mind the importance and the impact of implementing the requirements of the new version of the ISO 9001:2015 standard, it was deemed necessary to create a model of risk management based on the framework provided by the ISO 31000:2009 standard which would be built on the established correlation between the components of the new ISO 9001:2015 structure (Annex SL), the elements of the process-based risk approach and the types of risk viewed from the companies' perspective, in the case of this study, the financial services supplier.

Annex SL of the ISO 9001:2015 standard describes the structure which will define all subsequent management algorithms based on the ISO standards which will be provided in the future. This structure (comprised of 10 clauses) will be immovable, with the requirement that each clause will receive specific sub-clauses.

For the creation of the risk management model, we have selected clauses 4-10 from Annex SL, which were integrated alongside the stages which form the foundation of the risk-based thinking approach. All these were later on attached to the framework generated by ISO 31000:2009 for risk management (Table no. 2).

Clause 4 regarding the organisational context is necessary to determine the risks and opportunities which exist within markets, especially the financial sector. The companies providing financial services perform a continuous evaluation of these risks and opportunities to be able to provide consultancy to their clients. Because the consequences of the risk are not the same for all clients, with respect to this clause, risk-based thinking entails an evaluation of the risk profile of the investor by the company providing the financial services.

Investors can be placed into three main categories: investors with an aversion to risk, risk neutral investors, and investors who are drawn to risk. The investors, clients of the companies which provide financial services, can be both natural persons as well as legal entities. Determining the investment profile for older clients can be achieved by analysing their history of investments, and for investors who are new clients, an assessment can be performed by identifying their tolerance towards risk based on the answers they provide to specific questionnaires.

Table no. 2: The structure of the risk management model

Annex SL (ISO 9001: 2015)	Risk-based thinking approach	The ISO 31000: 2009 framework
4. Organisational context	Identifying risks; Analysing the risk profile	4.3. Designing the structure for risk management 4.3.1. Understanding the organisation and its specific context 4.3.2. Establishing risk management policies
5. Leadership	Analysing and prioritising risks	4.2. Authorisation and involvement 4.3. Designing the structure for risk management 4.3.3. Responsibility
6. Planning	Planning actions	4.3. Designing the structure for risk management 4.3.4. Integration within the organisational processes 4.3.5. Resources 4.3.6. Establishing internal communications and report mechanisms 4.3.7. Establishing external communications and report mechanisms
7. Support	Implementing the plan	4.4. Risk management implementation 4.4.1. Implementing the risk management framework 4.4.2. Implementing the risk management process
8. Operating		
9. Evaluating performance	Verifying the efficiency of the plan and improving the risk assessment process	4.5 Monitoring and reviewing the risk management framework
10. Improvement		4.6 The continuous improvement of the risk management framework

Source: personal concept through an adaptation based on ISO 9001:2015, ISO31000:2009 and risk-based thinking

Practically, in the field of financial investments, "risk-based thinking" is based on the concept of risk tolerance (an investor's capacity to take or avoid risks). Investors who are prone to accepting more risk are categorised under the profile of the investor who takes risks, while those who avoid risks are categorised under the profile of the investor with an aversion towards risk. Risk neutral investors are set on the border of risk tolerance.

An example of the degree of risk tolerance is illustrated in figure 1, in a two-axis system with two variables: the probability and impact of risk.

Acceptable risks are situated under the risk tolerance curve, whereas unacceptable risks are situated above this curve. The position of the curve with the system of axes is determined by the degree of risk acceptance by an investor (figure 2).

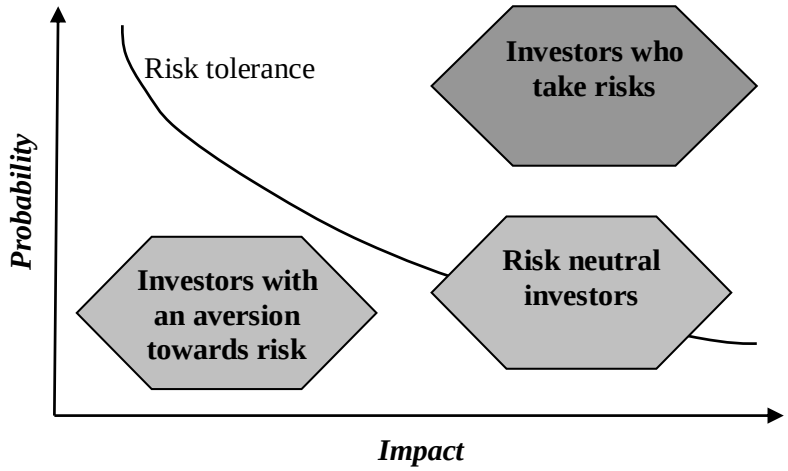

Figure no. 1: Risk tolerance of investors

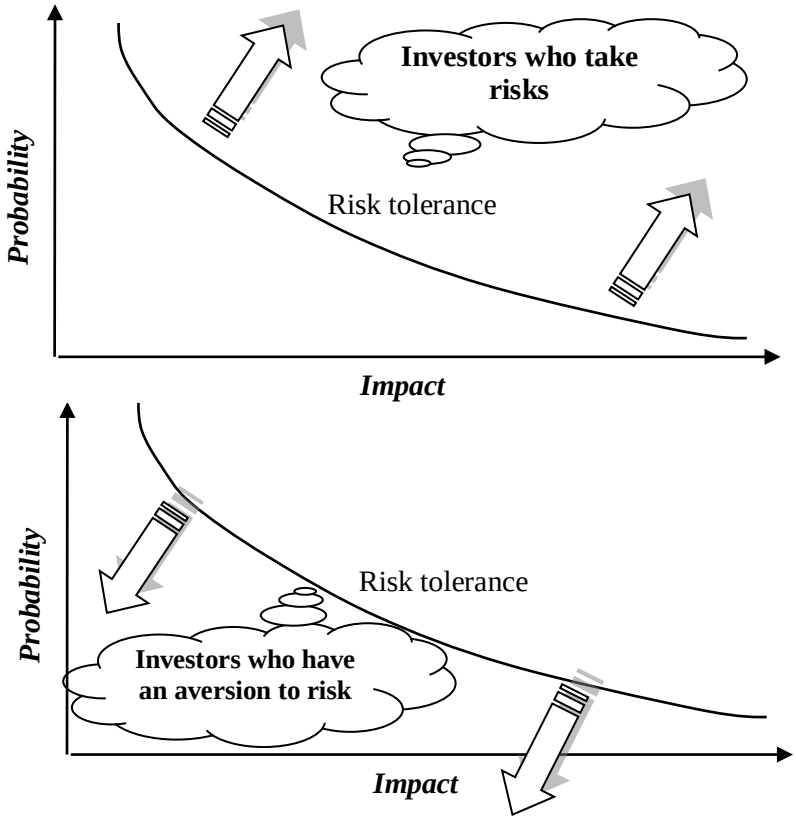

Figure no. 2: The tendencies of the investors who take risks and those of the investors who have an aversion to risk

While the risk-taking investor (speculator) accepts, larger risks compared to the average (moving the tolerance curve towards the upper right side of the figure), the investor who has an aversion towards risk avoids as much as possible risks (influencing the tolerance curve towards the bottom left side of the figure).

Within Clause 5 (leadership), there is an analysis and prioritising of risks based on the investor's risk profile. The investor will take the risks as they are explained by the company providing financial services. Within this procedure, an important role could be that of Risk Manager (Chief Risk Officer).

In Clause 6 (planning), the company supplying financial services will provide a plan of the method in which it approaches identified risks and opportunities.

Clauses 7 and 8 (support and operation) refers to the implementation of the plan established in the previous clause. The investor performs his planned investments in accordance with the plan agreed upon with the company supplying financial services. This ensures support and undertakes the technical aspects specific to investments.

In Clause 9 (assessing performance), the company supplying financial services monitors, measures, analyses and assesses the risks and opportunities together with the client investor.

Clause 10 entails the improvement of the financial risk management process. During this stage, a change can occur in the methods for risk assessment, as well as a re-evaluation of the investment profile as a result of subsequent changes in the risk tolerance curve.

Therefore, the proposed methodology includes a PDCA cycle (Plan, Do, Check, Act) applied to risks.

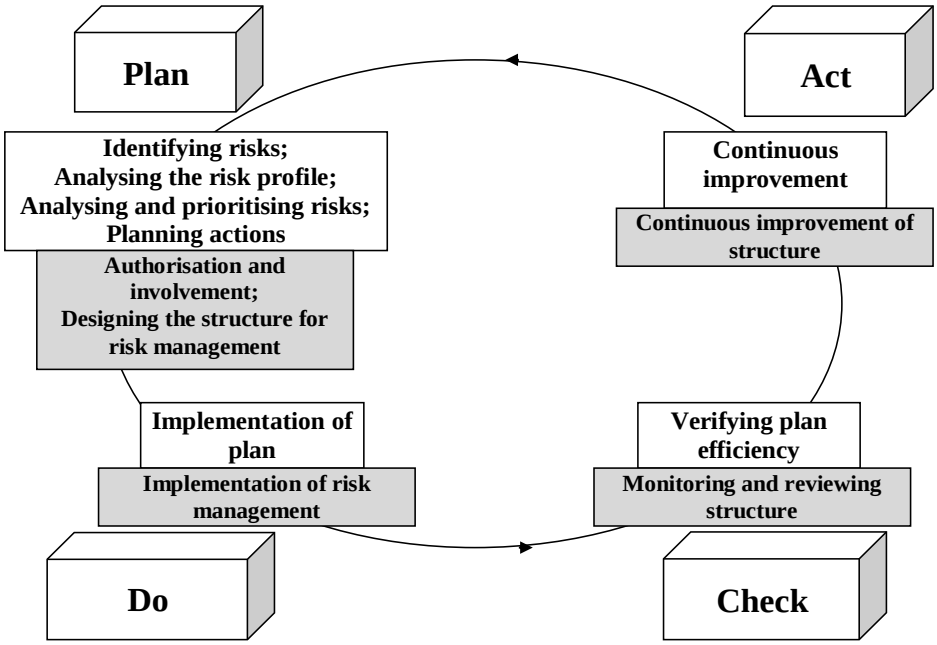

Figure no. 3: The PDCA cycle applied to risk-based thinking
Source: Personal concept adapted from BSI, (2015b)

Starting from the tolerance limit as established for each investor, we can adopt the response strategies in case of risk materialisation. They can be classified under four categories: strategies for negative risks (threats); strategies for positive risks (opportunities); strategies for both types of risks (threats and opportunities); strategies for unforeseen events;

a) The strategies for negative risks (threats) are avoidance, transfer and minimisation.

In the event of risk avoidance, the investor tries to eliminate the possibility of risk manifestation. The simplest way of avoiding risk is eliminating it. Bearing all this in mind, we must consider the fact that the profit is directly proportional to the risks taken. Eliminating risks will lead to the minimising of profit, thus adopting those financial instruments which entail no risks.

In the case of risk transfers, the responsibility of the risk is transferred onto another entity. The risk does not go away, only the responsibility is transferred should it materialise.

Risk minimisation entails bringing risk levels within an area of tolerance the investor is comfortable with. The company supplying the financial services will deal with either the probability or the impact to reduce risk levels so that they fall inside a limit of tolerance acceptable to the investor. A method of risk minimisation in the case of financial investments is represented by portfolio diversification.

b) The strategies for positive risks (opportunities) are capitalization, sharing and intensification.

Capitalisation deals with the opportunities the investor must seize. Through this, the uncertainties, which would otherwise impede opportunities, are eliminated. Sharing involves the distribution of positive risks (opportunities) onto another entity to adequately harness the opportunity. Intensification consists of changing the "size" of the opportunity by increasing the probability or the risk impact factor, identifying and maximising subsequent characteristics.

c) The shared strategy for both types of risks (threats and opportunities is acceptance. In the case of this strategy, the gravity of the risk is reduced, which makes the investor accept the risk without initiating strategies of avoidance or minimisation. Acceptance can be undertaken with both threats and opportunities, as there are two methodologies of operation associated with this strategy, passive acceptance and active acceptance.

Passive acceptance means the complete inaction in the event of risk identification. Many of the identified risks are passively accepted as they are too small to be considered (the quotation fluctuations of short-term financial instruments). The cost of modifying the plan is greater than the cost that would emerge when those risks would materialise. Passive acceptance means the acceptance of risks alongside a plan created to deal with the manifestations of risk (for example, establishing a stop loss).

d) The strategy for unforeseen circumstances applies in case of the emergence of certain risks that the investor has not identified in the risk management plan (financial crises, political crises which affect financial instruments, etc.). In this case, there are measures which can be undertaken to eliminate the unforeseen risks.

Risk management in financial services has acquired new dimensions because of the financial crisis of 2008-2010. Bier and Matthew (2009) show that in this area practices vary greatly from company to company and there are many companies that have not yet fully developed comprehensive risk management programs. There are methods and quantitative models but does not include clear procedures on how to act when emerging risks appear. In our opinion, it is necessary to introduce new models that should be more comprehensive and better integrated,

establishing some procedures for monitoring and reporting, as well as formal structures that at the Board of Directors level are capable to censor decisions of top management where assumed risks are not in the established risk strategy. Therefore, we consider it necessary to build a model of effective risk management based on ISO 9001: 2015 standard and ISO 31000: 2009 standard, a model that can generate clear procedures allowing identification, full understanding and taking neccessary actions in order to prevent and combat risks.

Conclusions

A risk management model is a structure based on which the strategy of the corporation must be constructed, bearing in mind the fulfilment of performance objectives and the constant monitoring of activities and processes. The new version of the ISO 9001:2015 standard, applicable from 2018, represent a major opportunity to forge an integrated system of performance management, through the creation of significant ties between quality management and continuous improvement, on the one hand, and corporate risk management on the other hand.

To cope with the changes imposed by the new version of the 9001 ISO standard, organisations must prepare for the adaptation of the quality management system with the purpose of meeting the new demands and transitory deadlines. The main objectives of ISO 9001 are and always have been providing increased trust in our organisation's ability to constantly provide goods and services which lead to increased customer satisfaction. The uncertainty regarding the achievement of these objectives has led to the explicit introduction of the notion of "risk" and the expression "risk-based thinking" from the perspective of ISO 9001:2015. The concept of risk has, since the beginning, been implied in ISO 9001 but had never been explicitly formulated. Risk-based thinking as defined by ISO 9001:2015 is a type of thinking every individual performs automatically, most of the times on a subconscious level. Risk is inherent in all the aspects of a quality management system. Risk exists in all the systems, processes and functions of an enterprise. Risk-based thinking entails that these risks should be identified, taken into consideration during the course of the planning and utilisation of the quality management system. Following this new revision, ISO establishes the foundation for the entire system of quality management based on this thinking.

Bearing in mind the financial service industry is exposed to a variety of risks, the risk-based thinking and the process-based approach, introduced by the ISO 9001:2015 standard, offered the opportunity of a better risk management solution on the part of financial services companies on behalf of their respective investors.

Through risk management in the case of financial services provided to client investors and in the case of companies providing financial services, it can reduce or increase risk based on the investors' risk profile.

Because of the introduction of risk-based thinking in the new version of ISO 9001:2015, we have deemed necessary the construction of a financial risk management model for the companies providing financial services, thus allowing better risk management for the benefit of clients, natural persons or legal entities, with the purpose of providing additional guarantees that risk is dealt with in accordance with strictly regulated, well-established procedures. The model also uses the ISO 31000:2009 standard, which offers the necessary foundation for the implementation of risk-based thinking as stipulated in the ISO 9001:2015 standard and the creation of the necessary system for the management of investment risk. The model can be applied by companies supplying financial services based on the risk profile of the investor, whether this client is a natural person or a legal entity, an old client or a new one.

The model also supplies a series of response strategies in the case of risk materialisation. The benefits of the model are significant as it offers a clear framework, procedures, courses of action, risk evaluation methods, all these being based on the provisions of the ISO 9001:2015 and 31000:2009 standards, in addition to an organic integration via the PDCA cycle. The model can be expanded and improved through the integration of methods of risk evaluation in the process.

References

Aebi, V., Sabato, G. and Schmid, M., 2012. Risk Management, Corporate Governance, and Bank Performance in the Financial Crisis. *Journal of Banking and Finance*, 36(12), pp. 3213-3226.

Bechara, A., Damasio, A.R., Damasio, H. and Anderson, S.W., 1994. Insensitivity to future consequences following damage to human prefrontal cortex. *Cognition*, 50(1-3), pp.7-15.

Berg, T., 2014. *Playing the Devil's Advocate: The Causal Effect of Risk Management on Loan Quality*. [pdf] Bonn University working paper. Available at: <http://www.tobias-berg.com/download/CausalEffectRiskManagement_vSep2014.pdf> [Accessed 12 January 2017].

Bier, S.H. and Matthew, A.W. 2009. Risk Management Issues for Registered Investment Companies. *The Investment Lawyer*, 16(7), pp. 9-16.

BSI, 2015a. *Why ISO 9001:2015 is better for your business*. [pdf] Whitepaper. Available at: <http://www.bsigroup.com/Global/revisions/Why-ISO-9001-is-better-for-your-business-FINAL-Dec-2015.pdf> [Accessed 27 August 2016].

BSI, 2015b. *The importance of risk in quality management*. [pdf] Whitepaper. Available at: <http://www.bsigroup.com/LocalFiles/en-IN/Resources/ISO%209001/ISO-9001-Whitepaper-Risk-in-quality-management.pdf> [Accessed 29 August 2016].

Bureau Veritas, 2015. *ISO 9001:2015 – What are the main changes?* [pdf] Available at: <http://www.revision2015.com/iso-90012015-what-are-the-main-changes/pdf> [Accessed 30 August 2016].

Deysher, B., 2015. *A "Risk Based Thinking" Model for ISO 9001:2015*. [pdf] Available at: <http://rube.asq.org/audit/2015/01/a-risk-based-thinking-model-for-iso-9001-2015.pdf> [Accessed 23 August 2016].

Ellul, A. and Yerramilli, V., 2013. Stronger Risk Controls, Lower Risk: Evidence from U.S. Bank Holding Companies. *Journal of Finance*, 68(5), pp.1757-1803.

European Commission, 2006. *Directive 2006/73/EC of 10 August 2006 implementing Directive 2004/39/EC of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms*. [pdf] European Commission. Available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:241:0026:0058:EN:PDF> [Accessed 10 January 2017].

European Commission, 2006. *Directive 2006/43/EC on statutory audits of annual accounts and consolidated accounts*. [pdf] European Commission. Available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1485109084580&uri=CELEX:32006L0043> [Accessed 10 January 2017].

Financial Stability Board (FSB), 2013. *Thematic Review on Risk Governance*. [pdf] FSB. Available at: <www.financialstabilityboard.org/publications/r_130212.pdf> [Accessed 18 January 2017]

Ganzach, Y., 2000. Judging risk and return of financial assets. *Organizational Behavior and Human Decision Processes*, 83(2), pp. 353-370.

Gilliam, J., Chatterjee, S. and Grable, J., 2010. Measuring the Perception of Financial Risk Tolerance: A Tale of Two Measures. *Journal of Financial Counseling and Planning*, 21(2), pp. 30-43.

Hunt, L., 2014. *ISO 9001:2015 - Understanding the Key Changes*. [pdf] Lorri Hunt & Associates Inc. 2014. Available at: <http://foro-internacional-de-la-calidad.icontec.org/memorias/CONFERENCIAS/JUEVES%20AGTO%2028/17.%20%20JV%20-%20ACTUALIZACION%20ISO%209001%20-%20LORRI%20JUNT-3.pdf> [Accessed 18 August 2016].

ISO, 2009. *ISO 31000:2009 Risk management — Principles and guidelines*. [pdf] Available at: <https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en> [Accessed 25 August 2016].

ISO, 2015. *Risk-based thinking in ISO 9001:2015*. [pdf] Available at: <http://www.iso.org/iso/iso9001_2015_process_approach.pdf> [Accessed 25 August 2016].

Jodkowski, L., 2015. Possibilities and Methods of Risk Assessment under ISO 9001: 2015. *International Journal of Managerial Studies and Research*, 3(10), pp. 14-23.

Kashyap, A.K., 2010. *Lessons from the Financial Crisis for Risk Management*. [pdf] Financial Crisis Inquiry Commission. Available at: <http://faculty.chicagobooth.edu/anil.kashyap/research/papers/lesson_for_fcic.pdf> [Accessed 14 January 2017].

Keys, B.J., Mukherjee, T., Seru, A. and Vig, V., 2009. Financial Regulation and Securitization: Evidence from Subprime Loans. *Journal of Monetary Economics*, 56(5), pp.700-720.

Kymal Chad, Reid R. Dan, 2015. *Risk Based Thinking and ISO 9001:2015*, [online] Quality Digest. Available at: <http://www.qualitydigest.com/inside/quality-insider-article/082115-risk-based-thinking-and-iso-90012015.html> [Accessed 2 September 2016].

Hutchins, G., 2014. Risk management & ISO 9001:2015. [pdf] Available at: <http://insights.cermacademy.com/files/2014/04/AmCon-Presentation1.pdf> [Accessed 2 September 2016].

Landier, A., Sraer, D. and Thesmar, D., 2009. Financial Risk Management: When Does Independence Fail? *American Economic Review*, 99(2), pp. 454-458.

Linciano, N. and Soccorso, P., 2012. *Assessing investors' risk tolerance through a questionnaire*, Discussion papers, Consob, July 2012.

Lingel, A. and Sheedy, E.A., 2012. The Influence of Risk Governance on Risk Outcomes - International Evidence. *Macquarie Applied Finance Centre Research Paper No. 37*. [e-journal]. http://dx.doi.org/10.2139/ssrn.2187116

Loth, R., 2016. 5 Ways to Measure Mutual Fund Risk. Investopedia. [online] Available at: <http://www.investopedia.com/articles/mutualfund/112002.asp> [Accessed 4 September 2016].

Lucarelli, C. and Brighetti, G., 2010. *Risk Tolerance in Financial Decision Making. The economics and the neuroscience perspective*, London: Palgrave Macmillan.

Lucarelli, C. and Brighetti, G., 2011. Risk Tolerance in Financial Decision Making, London: Palgrave Macmillan.

Management Solutions, 2014. *Model Risk Management Quantitative and qualitative aspects.* [pdf] Available at: <https://www.managementsolutions.com/sites/default/files/publicaciones/eng/Model-Risk.pdf> [Accessed 17 January 2017].

Marinelli, N. and Mazzoli, C., 2010. The Traditional Approach to Evaluate the Risk Tolerance of Investment Decisions, London: Palgrave Macmillan.

Mertz, C.K., Slovich, P. and Purchase, I.F.H., 1998. Judgments of chemical risks: Comparison among senior managers, toxicologists, and the public. Risk Analysis, 18(4), pp.391-404.

Miccolis, J., 2000. *Enterprise Risk Management in the Financial Services Industry: Still a Long Way To Go*. [pdf] Available at: <http://www.tuv-sud.com/uploads/images/ 14153343015405984816l3/tuv-sud-navigating-iso-9001-2015.pdf> [Accessed 3 January 2017].

Nowak, M. and Wójtowicz, L., 2015. Risk management based on ISO 31000. *Central european review of economics & finance*, 7(1), pp.51-60

NQA, 2015. *ISO 9001:2015 Transition gap analisys*. [pdf] Available at: <https://www.nqa.com/Nqa.com/media/PDF-Download-Documents/NQA-ISO-9001-2015-Gap-Analysis-Document-Oct-15.pdf> [Accessed 24 August 2016]

Office of the Comptroller of the Currency (OCC) and Board of Governors of the Federal Reserve System (FED). 2012. *Supervisory Guidance on Model Risk Management*. [pdf] Available at: <https://www.occ.treas.gov/news-issuances/bulletins/2011/bulletin-2011-12a.pdf> [Accessed 16 January 2017].

OECD, 2014. *Risk Management and Corporate Governance*. Corporate Governance, OECD Publishing.

Pergler, M., 2012. Enterprise risk management: What's different in the corporate world and why. [online] McKinsey Working Papers on Risk, Number 40. Available at: <http://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/risk/working%20papers/40_whats%20different%20in%20the%20corporate%20world.ashx> [Accessed 16 January 2017].

Saunders, M., Lewis, P. and Thornhill, A., 2009. Research Methods for Business Students. 5th ed. Harlow: Pearson Education Limited.

Slovic, P., 2000. *The perception of risk*. London: Earthscan Publications Ltd.

Stulz, R.M., 2016. Risk Management, Governance, Culture, and Risk Taking in Banks. *Economic Policy Review*, 22(1), pp.43-59.

Tale, N.N., 2005. *Fooled by Randomness: The Hidden Role of Chance in Life and in the Markets*. Random House Trade Paperbacks.

TUV SUD, 2015. *Navigating ISO 9001:2015 Understanding why the new ISO 9001 revision matters to everyone*. [pdf] White paper. Available at: <http://www.tuv-sud.com/uploads/images/14153343015405984816l3/tuv-sud-navigating-iso-9001-2015.pdf> [Accessed 1 September 2016].

Tseros, H., 2015. *The new ISO 9001:2015 Standard. Overview of Changes*. [pdf] Available at: <https://www.wmo.int/aemp/sites/default/files/WMO-TT-QMF-4-AI12-FromISO 2008to2015.pdf> [Accessed 27 August 2016].

Winters, Jr. R.E., 2014. *A Review ISO 9001:2015 Draft - What's Important to Know Now*. [online] Available at: <http://www.asrworldwide.com/images/ Quality_Registrar/ Presentations/ISO-Review/2015_ISO_9001_Review_Mar2014.ppt> [Accessed 15 August 2016].

Zuckerman, M., Kolin, E.A., Price, L. and Zoob, I., 1964. Development of a sensation seeking scale. *Journal of consulting psychology*, 28(6), pp.477-482.