OPERATIONAL RISK MANAGEMENT IN BANKS AND INTERNAL AUDIT FUNCTION ROLE IN OPERATIONAL RISK MANAGEMENT

CEM OĞRAŞ

107673022

İSTANBUL BİLGİ ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

BANKACILIK VE FİNANS YÜKSEK LİSANS PROGRAMI

ADVISOR: Prof. Dr. CEMAL İBİŞ

2010

OPERATIONAL RISK MANAGEMENT IN BANKS AND INTERNAL AUDIT FUNCTION ROLE IN OPERATIONAL RISK MANAGEMENT

CEM OĞRAŞ

107673022

Tez Danışmanının Adı Soyadı (İMZASI) :
Prof. Dr. Cemal İbiş

Jüri Üyelerinin Adı Soyadı (İMZASI) :
Prof. Dr. Oral Erdoğan

Jüri Üyelerinin Adı Soyadı (İMZASI) :
Kenan Tata

Tezin Onaylandığı Tarih :

Toplam Sayfa Sayısı: 71

Anahtar Kelimeler (Türkçe)	Anahtar Kelimeler (İngilizce)
1) Risk Yönetimi	1) Risk Management
2) İç Denetim	2) Internal Auditing
3) Operasyonel Risk Yönetimi	3) Operational Risk Management
4) Basel II	4) Basel II
5) Bankacılık Riskleri	5) Banking Risks

OPERATIONAL RISK MANAGEMENT IN BANKS AND INTERNAL AUDIT FUNCTION ROLE IN OPERATIONAL RISK MANAGEMENT

CEM OĞRAŞ

107673022

Tez Danışmanının Adı Soyadı (İMZASI) : **Prof. Dr. Cemal İbiş**

Jüri Üyelerinin Adı Soyadı (İMZASI) : **Prof. Dr. Oral Erdoğan**

Jüri Üyelerinin Adı Soyadı (İMZASI) : **Kenan Tata**

Tezin Onaylandığı Tarih :

Toplam Sayfa Sayısı: 71

Anahtar Kelimeler (Türkçe)

1) Risk Yönetimi
2) İç Denetim
3) Operasyonel Risk Yönetimi
4) Basel II
5) Bankacılık Riskleri

Anahtar Kelimeler (İngilizce)

1) Risk Management
2) Internal Auditing
3) Operational Risk Management
4) Basel II
5) Banking Risks

ABSTRACT

Operational risk defined as the loss making risk due to the internal processes, people or systems which are not suitable or not desired has become one of the most substantial problems that the banks faced in the recent years. Various researched were conducted related to the revealing the current state of the studies made to measure this risk type or this risk.

In this study, it is aimed to determine globally the internal audit function role of the banks in operational risk management and to assess the quality of related implementations in Turkey. The role of the internal audit function has been stated under operational risk management framework. In the last section of the study, the functions of a private bank's audit department operating in Turkey have been emphasized under the operational risk management framework.

In the conclusion of this study, it has been told that an efficient operational risk management will support and strengthen the internal control mechanism of the banks, but in order to achieve this, internal audit function is required to monitor all processes closely about the systems applied for operational risk management.

In the theoretical part of the thesis, upon the provision of the general information about the operational risk management and internal audit, a sample Turkish bank has been analyzed in the implementation section, and suggestions have been given to the role of the internal audit department in operational risk management.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AMA : Advanced Measurement Approach

ASA : Alternative Standardized Approach

ATM : Automated Teller Machine

BDDK : Bankacılık Düzenleme ve Denetleme Kurulu

BIA : Basic Indicator Approach

BIS : Bank of International Settlements

BRSA : Banking Regulatory and Supervisory Authority

CAR : Capital Adequacy Ratio

COSO : Committee of Sponsoring Organizations

CR : Credit Risk

EI : Exposure Indicator

EL : Expected Loss

KORI : Key Operational Risk Indicator

KRI : Key Risk Indicator

LGE : Loss Given Event

MR : Market Risk

OECD : Organization for Economic Co-operation and Development

OPVaR : Value at Operational Risk

OR : Operational Risk

PE : Probability Equivalence

UK : United Kingdom

USA : United States of America

VaR : Value at Risk

1. INTRODUCTION

The Basel Committee defined a set of principles for the banks in the document “Sound practices for the management and supervision of operational risk”. This document can be called as the manual of the internal auditors for supervising the operational risk management. The second principle of the document mentions that for verifying the effective implementation of operating procedures and operational risk strategy banks need qualified internal auditors. The board of directors is responsible to ensure that the internal audit staff is competent and properly trained. As an example, if the internal auditors don’t have the necessary competencies, the board of directors can even give the decision of outsourcing the audit function. It is very important to maintain the independence of the audit function during the above mentioned actions.

In general, the audit function should not give managerial decisions. Auditors may provide valuable recommendations for operational risk management but they should not have directly the operational risk management responsibilities. For instance, in Turkey, it is common that the internal audit functions of small banks are responsible for developing the operational risk management program. These applications may corrupt the independence of the internal audit function especially if the audit function is required to validate the process they had developed.

On one hand for internal audit function, it is important to supervise the operational risk management function appropriately. On the other hand it is important for the operational risk management the supervision and independent recommendations of the internal audit.

Contributing a global overview of the operational risk management framework and systems from the perspective of internal audit function and assessment of the implementations in Turkey are the objectives of this

study. Within this objective, a sample Turkish bank case study was done and criticized the internal audit function role in operational risk management. Besides, this study contains theoretical infrastructure of operational risk management, internal auditing and real banking implementations which were discussed in the viewpoint of internal audit function role in operational risk management.

2. OPERATIONAL RISK MANAGEMENT IN BANKS

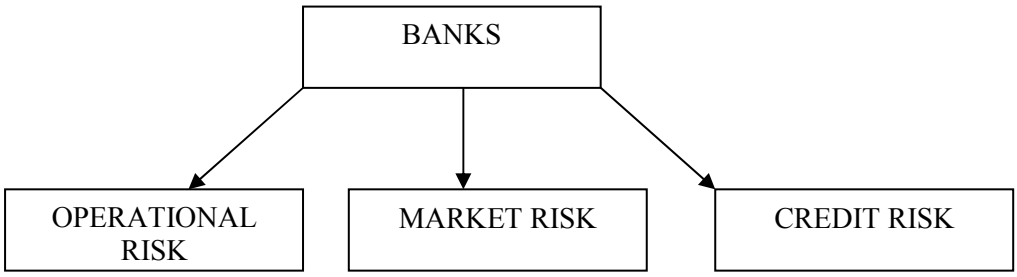
2.1 Definition of Risk and Types of Risks in Banking

Suggesting operational risk as an invention is not a realistic view. For many years banks have been aware of losses and uncertainties caused by defective information technology and infrastructure from fraud, from business disruption, and from legal liability. However after defining these risks under the concept of "operational risk" changed their location an status for managerial and regulatory purposes. Additionally a connection between operational risk and good corporate governance is made by Basel II. Therefore these risks should be positioned in a new space of regulatory, political and social expectations. After the invention of operational risk it is assessed concurrently with good governance and risk management. (www.jstor.org.library.bilgi.edu.tr/action/doBasicSearch?Query=operational+risk+management&wc=on, 2010)

The term risk has been defined by the Turkish Historical Society as "the danger of sustaining damage" Risk (http://tdkterim.gov.tr/bts/?kategori=verilst&kelime=risk&ayn=tam, 2009), in its most generalized definition, can be expressed as the failure to reach a certain target within a certain time interval and to sustain damage that one has to bear as a consequence of failure to reach the target. The concept of risk has been defined by BRSA (Banking Regulatory and Supervisory Authority) within the context of finance markets as the possibility for arises of a monetary loss or the economic benefit to decrease as a result of occurrence of an expense or damage (www.bddk.org.tr/WebSitesi/turkce/Mevzuat/Bankacilik_Kanununa_Iliskin_Duzenlemeler/1678BANKALARIN%20%C4%B0%C3%87%20S%C4%B0STEMLER%C4%B0%20HAKKINDA%20Y%C3%96NETMEL%C4%B0K%20(2).pdf, 2009).

In banking, risk types have been grouped into 3, namely operational risk, market risk and credit risk as shown in the below figure:

Figure 2.1: Types of Risks in Banking



Operational Risk: Operational risk generally covers all of non-financial risks (Numanoğlu, 2008). In other words, operational risk can be defined as all the risks other than sole credit risk and sole market risk. This comprehensive definition covers human faults, technology failures, insufficient controls and external factors as well as strategic and operational risks such as failure to give reaction to competitors and changing economic conditions.

Market Risk: Market risk is defined as the possibility for decrease in values of positions within or outside balance-sheets that the banks keep for purposes of purchase and sale, in interest rates, in the prices of commodities and share certificates, which occur by reason of changes in foreign exchange rates (www.bddk.org.tr/WebSitesi/turkce/Raporlar/Bankacilik_Sektoru_Risk_Degerlendirme_Raporlari/302Risk_Raporu_haziran2005.pdf, 2009).

As it can be understood from these definitions, there are three different types of risks, namely, interest rate risk of market risk, liquidity risk, and exchange rate risk.

Credit Risk: According to Süer (2002) Credit risk can be defined as failure of the debtor (bank customer) to pay its loan which has been extended to it as per an agreement in due time or at all for various reasons, in violation of the conditions of the agreement. As a result, credit losses occur. Loan risk can be reviewed under two types. These are:

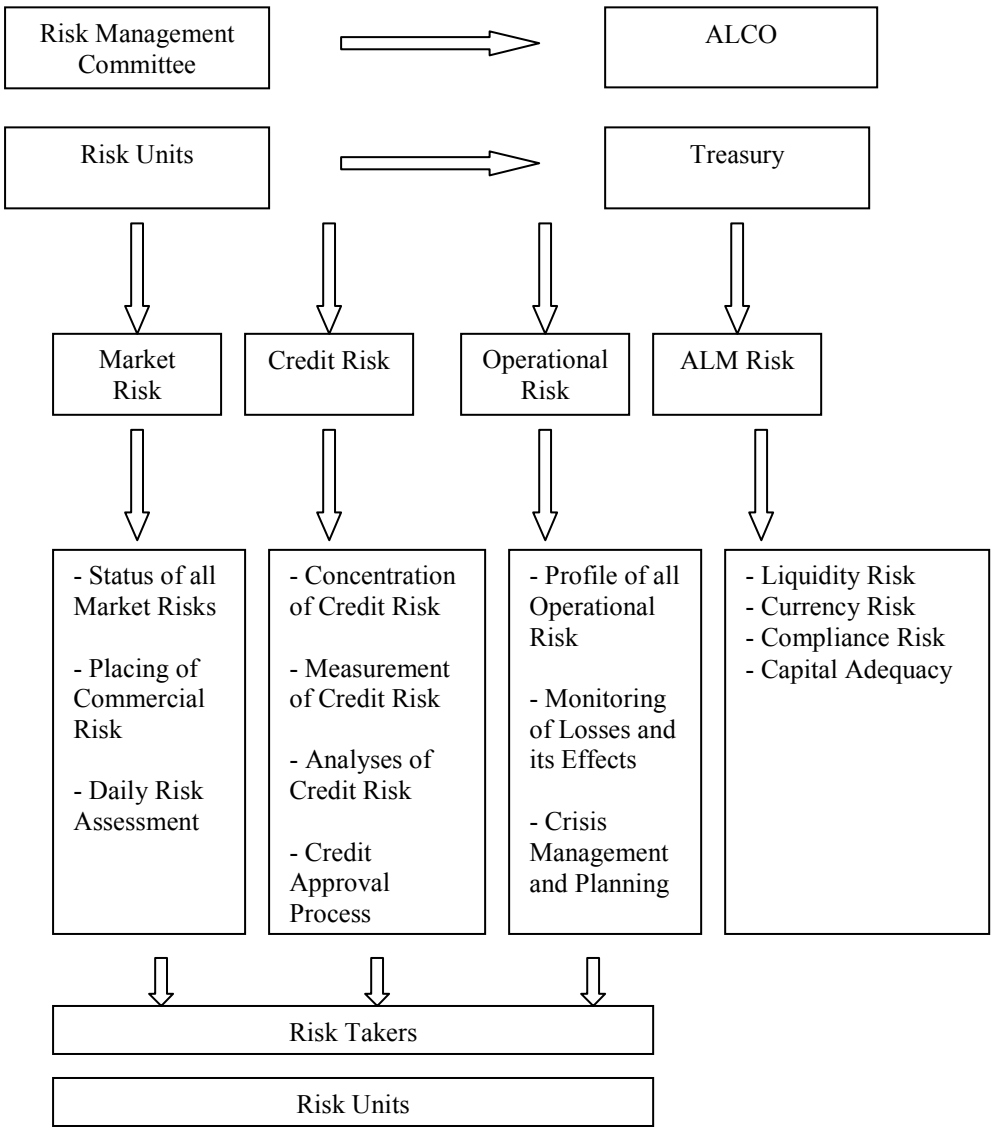
• **Customer or Credibility Risk:** The risk that the real persons and/or legal entities which have been extended loans by the bank cannot repay the outstanding loan debts.

• **Loan Risk Undertaken As a Result of Alternative Transactions:** The risks that arise out of instruments of banks such as foreign exchange transactions, financing of foreign trade, swap transactions, bills, options, derivatives, guarantees and bailments.

2.2 Risk Management in Banking System

Risk management in banking system is the mechanism in respect of procedures of determining standards, informing, compliance assessment, decision-making and implementation that are constituted with an aim to monitor, control and when necessary change the risk-revenue structure of future cash flows of a bank, quality and correspondingly, the quality and level of activities. The risk management framework is shown at the belove figure:

Figure 2.2: Risk Management Framework (Alkin, Savaş &Akman, 2001)



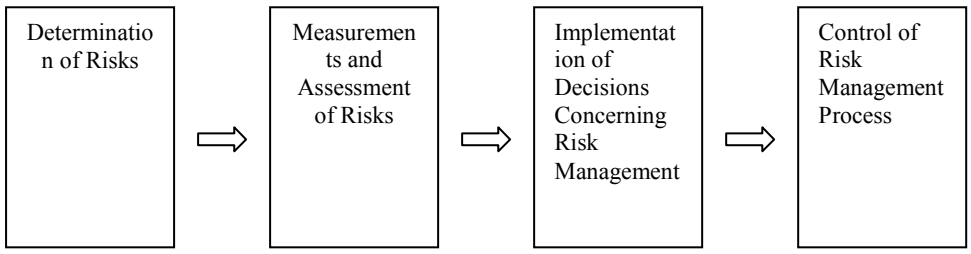
Nevertheless, risk management is an approach, a management philosophy which associates risk, revenue and capital, which establishes the most appropriate balance among them. It is necessary that the risk management systems that need to be set up fort its purpose should define the risks of the bank well, measure them accurately and on time, continuously monitor them and provide the largest data base to the

decision-making process in this respect, including pricing (www.makalem.com/Search/ArticleDetails.asp?nARTICLE_id=422, 2009).

2.2.1 Risk Management Process

As it can be understood from various definitions of risk management, it is observed that it is a process. This process is made up of the following stages;

Figure 2.3: Risk Management Process



• **Determination of risks:** Determination of the risks that the bank is/may be exposed to and classification of each of these risks in a certain manner.

• **Measurement and assessment of risks:** It is comprised of analysis by the bank of these risks that it has classified using various tools. Banks subject the results of these analyses to assessment with an aim to constitute a risk management strategy.

• **Implementation of decisions concerning risk management:** We can define it as the stage in which the banks form up risk management strategy, plan, program and procedures according to analyzed risk assessments.

• **Control of risk management process:** It is assessed whether the plans and programs that are made available and the strategies that are developed are effective in eliminating and mitigating the risks.

2.2.2 Purposes of Risk Management in Banking

The main implementation purposes of risk management in banks are protection of capital, increase of profitability and shareholders' value. Its prioritized target is to measure in advance the size of the damage that the banks may encounter under extraordinary circumstances experienced by the markets. Besides these fundamental targets, other risk management purposes are (www.makalem.com/Search/ArticleDetails.asp?bWhere=true&nARTICLE_id=403, 2009);

- To increase the quality of the knowledge regarding the risks,
- To accept the risks at the portfolio level,
- To measure and classify the risks and performances,
- To ensure consistency among risks taken and strategic objectives,
- To ensure effective and efficient management processes and procedures,
- To manage the risks from a control perspective,
- To optimize capital resources.

2.2.3 Evolution of Risk Management in International Markets

Evolution of risk management understanding in international markets has started much before than that in our country. Along with the breakdown of Bretton Woods system in 1970s, world markets witnessed circulation of more than one currency rather than a single currency. Emergence of these different currencies caused capital movement in the world markets and this caused the market to gain depth and led to arise of new instruments. Furthermore, rapidly developing technology caused international markets to stay open continuously, and realization of day-long

financial transactions. With the increase in competition as a result of these developments financial institutions have started to research and analyze financial instruments and their markets for purposes such as not allowing others to grab their market shares and to make more profit and to increase their shares in the market. This led to the emergence of the concept of risk.

With the emergence of the risk concept, international institutions were established in order to eliminate the risks and to mitigate their effects and various arrangements were made through these institutions. The most effective organization among these institutions is BIS. (Bank of International Settlements) Although the regulations made by this institution are not binding, they are accepted as basic in international markets and our country and the countries try to adapt themselves to these regulations.

2.2.4 The Basel II Capital Accord

The Basel I Accord dated on 1988 was prepared by the Banking for International Settlements (BIS) Committee, pertinent to the determination of the capital standards for the banks operating internationally, and became a general capital adequacy standard for all world countries and banks from the date of its announcement. However, upon the application of this Accord, some problems started to reveal. These problems are inadequacy of the capital standard in risk measurements since it uses credit risk as the basis, along with failure to measure the risk in the required sensitivity because the applied risk measurement method required to be applied by all banks, and taking OECD membership as the basis for fundamental loan risk criteria.

In 1999, the Basel Committee prepared a new capital adequacy draft. This Draft known as the Basel II Capital Accord has more extensive risk sensitivity and measurements. The Basel II supports an advance risk management by using three structural blocks supporting each other. It is of first priority for the banks to determine the material risks in realistic manner

and to preserve the capital level to meet this. The Basel II states that only capital requirements shall not be adequate to provide the safety environment in the banking system or to have required capital adequacy and risk management, and a strong audit system having early intervention system and effective market discipline shall be complimentary to the capital requirements (www.bddk.org.tr, 2009).

It was become a necessity to define the banking capital adequacy standard again and more extensively due to the failure of the banks defined under Basel I to include the rapid changes in the financial markets in their current methods used in the measurement of the credit risk exposure on the banks and market risk and to consider the interbank structuring in addition to quality differences and other reasons specified above. Therefore, the Basel Committee established a formal negotiation platform for the new capital standard in 1999 mentioned as the Basel II, and presented the discussion subjects to the relevant parties on the Internet. This draft was undergone a number of substantial revisions in the recent years pursuant to the recommendations and critics received. It is expected that the Basel II standard will be applied from the beginning of 2007.

CAR = Owner's Equity / (CR+MR+OR)

CAR: Capital Adequacy Ratio

CR: Credit Risk

MR: Market Risk

OR: Operational Risk

Operational Risk (OR) was included to the banking risk types defined by the Basel II. Besides, it was allowed to measure the credit and market risks exclusively which had been measured with standard methods being the same for each bank. The other cornerstones of the Basel II require proactive and effective supervision by the public authorities and

presentation of detailed information by the banks to the market in risk activities and risk management issues.

The Basel II Accord consists of three structural blocks. These three structural blocks are minimum capital requirement, public supervision and market discipline, and the following table indicates the contents and targets of each structural block.

Table 2.1: Basel II Structural Block (Candan & Özün, 2009)

Structural Block	
1. Minimum Capital Requirement	Internal Audit of Bank: Measurement, monitoring and control of the risks by banking authorities
2. Public Supervision	Audit by the Public Authority: Audit by the Banking Supervision and Regulation Agency related to the effectiveness of the risk management and internal audit by the bank
3. Market Discipline	Market Audit: includes the supervision of the Bank by the market authorities.

2.2.5 Development of Risk Management in the Turkish Banking System

Along with the process of marketisation which increased as of 1980s in Turkey, banking sector has entered into a development process. Marketisation process helped the development of the banks but at the same time caused rapid increase of inflation, interest rates and foreign exchange rates. In this manner, the banks had to evaluate different instruments well in order to be able to protect their current statuses and to compete with external competition. However, interest rates that increased upon transition to market economy also increased the borrowing needs of the public sector. Banks which started to finance the public debts which had low risk and high

revenue, started to obtain high amounts of profit. With the influence of this, during these years, studies of risk management for banks were found unnecessary and there was lack of sufficient studies in this respect. International arrangements for risk management were insufficient. This recklessness in the field of risk studies has started to disappear in 1997 with the crisis in Southeastern Asia and as of November 2000 and February 2001 crises in our country. With the effect of these crises, a new period has begun in the Turkish banking sector. Many changes were made in the financial markets and the banking sector. This process which started after making amendments in the banking law continued with the formation of the Banking Regulatory and Supervisory Authority which is the authorized institution for regulating and supervising the banking market.

Risk management was for the first time regulated in the banks law numbered 4389 which became effective on 18 June 1999 and the banks were held responsible for establishing an effective internal audit system that conforms to the scope and nature of their activities, and that will be specified in a regulation to be issued by the authority, with an aim to monitor and inspect the risks encountered by the banks during their transactions. Within this framework, with the "Regulation concerning Establishment of Internal Audit and Risk Management Systems in Bank and their Activities" that was published on 8 February 2001 by the Banking Regulatory and Supervisory Authority and that conformed to the international arrangements, an important step was made for the Turkish banking sector. This regulation determined the principles and procedures concerning the internal audit systems and risk management systems that would be set up by the banks in order to monitor and control the risks they encounter and also mentioned the establishment of the technological infrastructure (Candan & Özün, 2009).

A road map was set up by the Banking Regulatory and Supervisory Authority with an aim to adapt the arrangements made by BIS. The studies

for making the banking system compatible with these arrangements as per a specific program are still continuing.

In Article 29 of the new Banking Law accepted on 19 October 2005, risk management is expressed as follows: “Banks are responsible for establishing and operating an internal control, risk management and an internal audit system that covers all the branches and subsidiaries subject to consolidation, that is compatible with the scope and nature of their activities with an aim to monitor the risks they sustain and to control them”.

2.3 Operational Risk and its Management

The technological attempts made within the last 20 years have played an important role in the development of financial markets and finance engineering. This allowed formation of particularly derivative types and other financial innovations. In this manner, skills of the banks to evaluate the risk profiles and actively manage them have developed and this made risk management process multi-faceted and complex. Along with the complexity of the transactions, the speed of completion of such transactions and the need for data increased. In parallel to these developments, the dependence of financial institutions to technological systems and key personnel has become more apparent (www.tkgm.gov.tr/turkce/dosyalar/diger%5Cicerikdetaydh338.doc, 2009).

Increasing complexity of the markets has started to cause the institutions to make more faults. Furthermore, as a result of the faults made by institutions such as Deutshe Bank, eBay, Barings, Daiwa, Procter8Gamble etc. which operate in the international financial markets, they incurred significant damages. This shifted the attention to a new type of risk, which is Operational Risk, and increased its importance. After all these, operational risk has taken its place in the world of finance as a separate field with the arrangements of BIS. The following figure indicates the most known operational risk incidents in the world:

Table 2.2: Examples for Operational Risk Losses

(www.makalem.com/Search/ArticleDetails.asp?nARTICLE_id=1294, 2009)

Corporation	Event	Year	Loss Amount($ Billion)
Daiwa Bank, New York	Unauthorized Bond Transactions	1984-95	1,100
Sumitomo Corp, London	Unauthorized Transactions, Fraud, Counterfeiting	1986-96	1,700
UK Life Insurance Sector	Insurance Premium Forgery	1988-94	18,000
Standard Chartered, India	Unlawfulness in Bombay Stock Exchange	1992	400
Credit Lyonnais	Weak Credit Controls	1980-90	29,000
USA Banks, Firms and Retailers	Corruption in Cheques	1993	12,000
London Stock Exchange and its Members	Breakdown of TAURUS System	1993	700
Kidder Peabody	Bond Trade, Inadequate Internal Controls	1994	200
Procter&Gamble	Managerial Faults	1994	157
Morgan Grenfell	Incorrect Accounting Records	1990	640
Orange Country	Bond Trade, Inadequate Managerial Controls	1994	1,700
Baring, Singapore	Inadequacy in Derivative Instruments and Segregation of Duties	1995	1,600
Deutsche Bank, London	Unauthorized Investment Decisions	1996	600
eBay	Technological Problems	1999	5,000 (Decrease in Market Value)
Enron, USA	Fraud and Uncontrolled Derivative Transactions	2001	60,000 (Decrease in Market Value)
Andersen, USA and its World Operations	Inadequate Internal Controls	2001	6,000
Imar Bank	Unauthorized Transactions, Fraud, Counterfeiting and Inadequate Controls	2001	6000 (Embezzlement)

When the evolution of operational risk is reviewed within the framework of risk management,

• It was evaluated only within Credit Risk under the framework of Credit Risk Management in 1970s,

• It was evaluated within Market and Credit Risk under the framework of Financial Risk Management in 1980s,

• It took place under a separate heading under the framework of Company-wide Integrated Risk in 1990s and 2000s.

2.3.1 Definition of Operational Risk

There is no common unanimously agreed definition of operational risk although it has a longer history.

BIS defines operational risk as “the risk to sustain damages as a result of inappropriate or non-functioning internal processes, people, systems or external effects”. In Turkey, Banking Regulatory and Supervisory Board, on the other hand, defines operational risk as; “the possibility to incur loss or damage as a result of ignorance of faults and irregularities due to problems in internal controls, failure of the bank management or personnel to act according to the deadlines and conditions, faults in the bank management, faults and problems in the information technology systems, as well as a result of natural disasters such as earthquake, fire or flood.” (www.bddk.org.tr/WebSitesi/turkce/Mevzuat/Bankacilik_Kanununa_Iliskin_Duzenlemeler/1678BANKALARIN%20%C4%B0%C3%87%20S%C4%B0STEMLER%C4%B0%20HAKKINDA%20Y%C3%96NETMEL%C4%B0K%20(2).pdf, 2009).

2.3.2 Types of Operational Risk

Operational risks have been divided into 4 groups, which are,

- Operational risks arising from people;
- Operational risks arising from system
- Operational risks arising from process;
- Operational risks arising from external factors. The types of these risks have been detailed below;

Operational risks arising from people: As defined in the work of Teker (2006), operational risks arising from people are the risks that arise as a result of inadequacy, or negligence of bank management and personnel or their ignorance or abuse of their duties or their intentional engagement in acts which are deemed as crime. For example, participation of bank's management in other initiatives without making a due review, extension of loans without taking guarantees and in excess of limits, inability to adapt the technological innovations to the bank, inability to keep pace with change, insufficient promotion of products and services, theft and fraudulent acts by the personnel, the personnel's failure to comply with the instructions or their violation of rules, the personnel's intentional prevention of the work, or their acting in bad faith can be evaluated within the scope of personnel risk.

Factors such insufficient knowledge or experience of the personnel, lack of motivation, excessive work load, irregular change of locations, unsuitability of the workplace or lack of order at the workplace can be listed as personnel risks (www.tkgm.gov.tr/turkce/dosyalar/diger%5Cicerikdetaydh338.doc, 2009).

Operational risks arising from system: These are the risks that occur by reason of technical problems and failures in computers and communication systems, virus problems, problems arising out of insufficient or outdated systems (www.tkgm.gov.tr/turkce/dosyalar/diger%5Cicerikdetaydh338.doc, 2009).

However, intentional acts by the personnel of the institution are evaluated as personnel risk, and intentional attacks made from outside the institution are evaluated as external source risks. In short, risks arising from non-intentional disruptions and insufficient are specified under this group.

As an example to system and technology risks, we may list the losses in the data, time and financial losses that arise as a consequence of

software and hardware failures, or inability of the computer systems to meet the demands of the customers.

Operational risks arising from process: These are the risks that arise due to lack of procedures in respect of processes related to the flow of activities of the organization or in respect of internal controls having the function of complementing the processes, or due to wrong planning of the existing procedures or inaccurate implementation of the same. The insufficiencies in the flow of information among internal units, non-existence of mechanisms in respect of powers, inability to determine the risks sustained by the organization and failure to adequately inform the employees of the risks are among factors causing these kinds of risks (Can, 2003).

Operational risks arising from external factors: According to Babuşcu (2005) operational risks that arise from external sources are the risks that occur solely due to external factors and that do not have any connection with the bank. As an example to these risks arising from external factors, attempts for robbery directed at the bank, attempts for fraudulent acts, acts of terrorism, natural disasters, wars can be listed. In addition, failure of the suppliers and outsourced contractors to comply with the criteria set out in the agreement, bankruptcy of the organizations from which services are procured, amendments made in the legislation, taking of decisions by governments that concern banks are also operational risks that arise from external sources. The factors leading to the external risks are shown in the following table:

Table 2.3: Factors Leading to the External Risks

Corruption	Irresponsible Local Managements	Excessively Large Projects
Nepotism	Undisclosed debts	Non Binding Financial Regulations
Bad Decisions related to the Business	Excessive Consumption Expenses	Foreign Banks with very high loan giving desire
Money Speculators	Low Interest Rates	Sectors diversified extravagantly
Real Estate Manipulations	Foreign Investors	Camouflaged Relations between the Government and Business World
Fraudulent Buyers/ Sellers	Financial Liberalization	Domestic Banks with very high loan giving desire

2.3.3 Measurement of Operational Risks

With the measurement of operational risks, gathering of unpredictable losses and damages and predictable losses and damages together, and formation of a data base for the organization, it was aimed to minimize the risks that could be sustained by the organization, with the experience gathered there from and estimations to be made for the future.

The stage of measurement of operational risks is comprised of a process formed up of sub-stages. Within this process, first of all, the data that have been entered in a specific order are gathered in a data base, and then these data are used to measure the operational risk, and finally, along with the assessment and reporting of these, the next stage of management process starts.

During the process of management of the operational risk, the stage of measuring the risk and calculating the capital required for the risk are the most complex and controversial stage as measurement of operational risk has always been a difficult job. The existence of many various risks, variety

of their effects and timeframes, difficulties in determining causal factors, harm to image is only some of them. The most difficult of these is the limitedness of the data regarding operational risks (www.makalem.com/Search/ArticleDetails.asp?nAUTHOR_id=162&sResultType=BrowseAuthor&sLetter=&sAuthorText=Aksel,%20%20Kaan&nPage=2&nOrder=2&ALLRESULTS=1883,493,503,2068,4426,436,426,1110,457,478,1563,495,432,2545,1562,4437&Sayfa=2&nARTICLE_id=1110, 2009).

The fundamental logic that lies behind the concept of measurement of the operational risk is actualization of the frequency and effect estimation regarding the future by using the data pertaining to the past. Therefore, we can say that most of the methods of estimation can generally be used for measurement of the operational risks (in the form of necessary assumptions) (www.makalem.com/Search/ArticleDetails.asp?nARTICLE_id=1294, 2009).

These methods (approaches) that are implemented for measurement of operational risks are gathered in two groups, namely "Quantitative — Qualitative Approaches" and "Top Bottom- Bottom Top Approaches". Other than these, there are also approaches of the regulatory authorities related to measurement of operational risks.

2.3.3.1 Loss Data Base

Basel Committee developed classifications of loss data by determining data classes in respect of the nature of loss along with the reason of arise of operational loss events. The reason is to be able to make objective risk measurement by way of expressing the losses in figures. The distance that has been covered in the loss data approach has not yet been covered in the causality approach. The approach that has been developed as regards loss data was first realized by the Operational Risk Working Group

which operates under the auspices of Institute of International Finance. According to this approach, data of loss have been classified into two groups, namely operational risk events and the effects of such events (www.bddk.org.tr/websitesi/turkce/Basel-II/1283MM_Opriskdata.pdf, 2009).

These loss types are comprised of the following.

1- Decreases in asset value,

2- Losses that arise from recovery,

3- Compensation of loss and returns,

4- Legal liability,

5- Penalties that are incurred by reason of failure to comply with the supervisory authorities and legislation

6- Losses that arise from assets and damages to assets.

Classifications made in respect of operational risk events with an aim to provide monotony in risk measurements have been shown below.

1- Internal Fraud

2- External Fraud

3- Employment Practices and Workplace Safety

4- Clients, Products, & Business Practice

5- Damage to Physical Assets

6- Business Disruption & Systems Failures

7- Execution, Delivery, & Process Management (www.bis.org/publ/bcbs107.pdf?noframes=1, 2009).

The following table indicates a sample of loss data of an operational risk event:

Table 2.4: Operational Loss Data

(www.riskcenter.com.tr/operasyonelrisk/operasyonelfiles/veritaban.pdf, 2009)

Information Field	Detail	Example
Loss Data Information		
Reference Number		1111
Personnel ID		36886
Personnel's Unit		Accounting Unit
Approval Unit		Risk Management
Description of Event		Internal Fraud in Customer's Accounts
Business Line		Retail Banking
Loss Event Type		Internal Fraud
Risk Source	System	X
	Process	
	Personnel	X
	External	
Place of Event	Unit	Antalya Branch
	Section	Antalya Region Management
	Region	Antalya Region
Date	Event Date	01.10.2006
	Detection Date	04.10.2006
Detection Type	Audit	
	Customer Complaint	X
	Personnel's Notice	
	Other	
Gross Loss		10500 USD
Coverage	Insurance	
	Law Court	
	Customer	
	Personnel	2000 USD
	Other	
Expected Coverage		8500 USD
Accounting Date		13.12.2006
Direct Effect	Financial Loss	
	Accounting Adjustment	
	Physical Damages	
	Loss of Revenue	
	Customer Loss Coverage	X

	Punishment	
Intangible Effects		Customer Complaints
	Open	
	Closed	
	Canceled	
Status of Event	Other	
Risk Management		
	Internal Control	Yes
Status of Audit	Internal Audit	Yes
	System Inadequacy	
	Authorization Violation	
	Reconciliation Deficiency	
	Process Violation	X
Control Weakness	Other	
Status of Investigation/Examination/Law Suit		Investigation
Management Decision		Ensuring Systematic Controls and Disciplinary Action
	Market	
	Credit	
Risk Type	Operational	X

2.3.3.2 Quantitative and Qualitative Risk Approaches

Quantitative approaches which are the second important dimension of assessment of operational risk are based upon value estimations as a result of subjective experiences which help reflecting the risk status in a systematic or non-systematic manner (www.tkgm.gov.tr/turkce/dosyalar/diger%5Cicerikdetaydh338.doc, 2009).

Quantitative operational risk measurement techniques can be listed as follows:

• **Causal Models:** It is the method of representing the physical world. Causal models that have been designed and implemented well can give very useful results for discovering the reasons lying behind the events. Causal Modeling is important for operational risk management and simple

quantification. Financial institutions must understand the root causes of operational risk and how they lead to loss events in order to change the capital allocation required under Basel II for operational risk. Furthermore causel modeling enables the inclusion of operational risk in the business decision processes, such as business process re-engineering, infrasturucture re-engineering, and infrastructure operation (www.jstor.org.library.bilgi.edu.tr/action/doBasicSearch?Query=operational+risk+management&wc=on, 2010).

• **Statistical Distributions:** They are used for determining the worst tendency that a specified risk can show in time. The most well-know of this technique is the Value at Risk (RMD-VaR).

• **Theory of Excessive Ends:** This theory is used for making the estimates that are provided for measurement of the risks in case of data insufficiency. It is frequently used in rare circumstances that occur in the insurance sector such as storms and earthquakes.

• **Artificial Nerve Networks:** They function by taking as basis the working mechanism of the human brain. The most important characteristic is that it is able to make relationships among data.

Qualitative approaches are those that are mostly based on probability calculations. Qualitative operational risk measurement techniques are as follows;

• **Process Review:** Before definition of risk, careful analyses of business processes should be made. Analyses must be made routinized with the operational risk management. For this, the first stage is to determine the business process criteria as a result of the analyses. Following this, personnel interviews, work flow charts and analyses should be implemented.

• **Assessment of Risks by Employees:** In this method, in cases where there are no data that will allow making of analyses, the risks need to be assessed by the employees. This assessment process is comprised of three stages. These are;

• Definition of operational risks,

• Determining basic resources of operational risks,

• Estimations of probability and effect levels regarding the risks

• **Causality Analysis:** It relates to determination of factors that influence occurrence of the risk by reviewing the results retroactively. Analysis techniques can be listed as follows;

• **Fishbone Technique:** Each potential problem is shown by an arrow and the relationship among the problems is expressed with the help of an arrow.

• **Fault Trees Analysis:** It focuses on big destructive events and tries to analyze the possible effects of the events that can be associated with the said event in the form of "and" and "or" from top to bottom.

• **Event Trees:** It aims to determine what could be the indirect effects of wrong management and how the problems can go out of control (www.makalem.com/Search/ArticleDetails.asp?nARTICLE_id=1294, 2009).

2.3.3.3 Top Bottom – Bottom Top Risk Approaches

Top to bottom approaches aim to specify target parameters in relation to the performance of the organization and to calculate the dimension of the risk on the basis of the effect of the operational risk factors on such parameters. This approach is generally formed up of stages such as determining target parameters, determining external and internal

risk factors that can influence this parameter, development of the model that will set out the relationship between the parameter and the risk factors and calculation of the dimension of the operational risk according to the variability observed in the target parameter.

Although top to bottom approaches are seen advantageous since they take into consideration the operational risk capital during the process of decision-making and since they are easy to implement and have a low cost; they are criticized, however, since they focus not on the factor that cause operational risks but on the effects of such factors on the target parameter, and therefore, they do not serve as a guide in respect of risk management. Examples to top to bottom approaches are; share certificate value models, revenue basis models, expense basis models, activity leverage models, scenario analyses and risk profile models.

Increase in the knowledge relating to simulation techniques of use of qualitative techniques in risk management and risk management units and formation of data bases in respect of damages that were incurred in the past caused these bottoms to top approaches to be widely used by financial institutions. The most basic parameters in relation to activities, such as assets and liabilities, resources and processes are determined in bottom to top approaches, and the effects of changes in these parameters on the main parameters such as net revenue are assessed. It is assumed that negative effects arise out of various risk factors or loss events.

This approach gives more accurate results since it deals with the risks on the level of the field of activities and branches of operation and since it uses data in respect of operational risk damage events. Examples to bottom to top approaches are; asset liability management, causal models, operational control lists and stress tests (Can, 2003).

2.3.4 Approaches of Calculation of Capital Requirement for Operational Risks

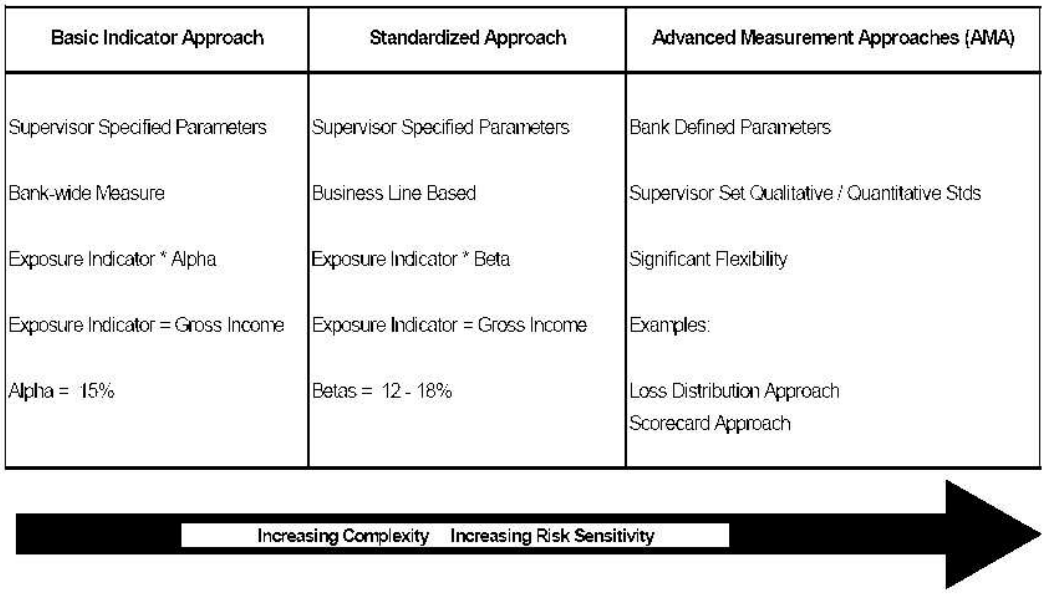
Operational risk can be devided into two types according to operational economic and mathematical characterization. First one is the risk of loss caused by the operating systems of the bank. It can be a failure in a transaction or investment, either due to an error in the back office (or production) process or due to legal considerations. Second one is the agency cost caused by the separation of a bank's ownership and management. In economics agency costs are recognized as a significant force. They have received significant study in the corporate finance literature as key determinants of the bank's capital structure and dividend policy(www.sciencedirect.com.library.bilgi.edu.tr/science?_ob=ArticleListURL&_method=list&_ArticleListID=1368171579&_sort=r&view=c&_acct=C000052709&_version=1&_urlVersion=0&_userid=1437276&md5=150c97e16ae0be8c816942e8865d09de, 2010).

Basel Banking Committee has suggested three different approaches for calculation of the capital amount that needs to be set aside for only the quantifiable part of the operational risk. As shown in the following figure, these approaches are;

- Basic Indicator Approach
- Standardized Approach
- Advanced Measurement Approaches

Figure 2.4: Approaches for Calculation of Capital Requirement for Operational Risks

(www.bos.frb.org/bankinfo/qau/presentations/2003/er5103.pdf, 2009)



2.3.4.1 Basic Indicator Approach

The simplest method that can be used for determining the capital to be made available for operational risks is Basic Indicator Approach (BIA). This approach is based on multiplication of a variable which shows the size of the operational risk with a coefficient that is determined (α- alpha). In this approach, the principle to use the gross income as the financial variable and to implement alpha coefficient as 0.15 has been adopted.

Here, gross income is comprised of provisions, security purchase-sale profit-loss in banking accounts, extraordinary items and net interest income excluding the income derived from insurance activities and net non-interest income.

BIA foresees that banks should, for their operational risks, keep a capital in an amount to be reached by taking the average of the last 3 years and to be calculated for each year as 15% of the gross income of the previous 3 years.

$Capital_{BIA} = [(BIS_{1.....n} \times \alpha)] / n$

$Capital_{BIA}$: Capital amount calculated with the Basic Indicator Approach,

$BIS_{1.....n}$: Annual Gross Income

α: Coefficient that is specified by the Committee as 0,15

n: Number of years in which the gross income was positive within the last three years

The numbers relating to any year in which the annual gross income was negative or zero must be kept outside both the numerator and the denominator. In this manner, in case the negative gross income distorts the Primary Structural Block capital amount of a bank supervisory authorities shall evaluate the implementation of suitable measures within the scope of Secondary Structural Block (www.bddk.org.tr/WebSitesi/turkce/Basel-II/1249Basel%20II%20Cevirisi-14102005-16_19.pdf, 2009). However, national regulatory authorities have brought a different approach to this matter. The national authority says that in calculation of the capital amount, if the gross income is negative, absolute value thereof can be used without looking at the sign of the gross income (www.tkgm.gov.tr/turkce/dosyalar/diger%5Cicerikdetaydh337.pdf, 2009).

Use of gross income as an indicator of the operational risk has brought with itself many criticisms. The point of focus of the criticisms against this approach is whether or not gross income can be an indicator of the operational risk. When the nature and characteristics of the operational risk are taken into consideration, it is seen that gross income cannot give an idea regarding the level of risk.

This indicator's capability of being suitable for all purposes and its applicability to all the banks in common despite all the deficiencies among the indicators that can be used as a risk indicator in this field helped this

indicator to be adopted. In addition, determination of α coefficient high encourages the use of approaches that are responsive to risk to mitigate the arising capital requirement (www.tkgm.gov.tr/turkce/dosyalar/diger%5Cicerikdetaydh337.pdf, 2009).

2.3.4.2 Standardized Approach

In standards approach activities of a bank are divided into eight different business lines. Each business line functions as an indicator which shows the gross income, business operations and activity scale and therefore, the possible scale of the operational risks in each business line.

Table 2.5: Standardized Approach Weight Rates

(www.bddk.org.tr/WebSitesi/turkce/Basel-II/1249Basel%20II%20Cevirisi-14102005-16_19.pdf, 2009)

Business Line	Beta Factor
Corporate Finance (β_1)	18%
Trading and Sales (β_2)	18%
Retail Banking (β_3)	12%
Commercial Banking (β_4)	15%
Payment and Settlement (β_5)	18%
Agency Services (β_6)	15%
Asset Management (β_7)	12%
Retail Brokerage (β_8)	12%

The liability to have capital for each business line is obtained by multiplying the gross income with a factor allocated to such business line (Beta factor). Beta is a coefficient which shows the current relationship in the sector between operational risk loss experience in a certain business line and the total gross income level for that business line. In the standardized approach, it should be noted that gross income is measured separately, for each business line, and not for whole of the activities of the institution; for example, the indicator value used in the corporate finance business line is the gross income created in the corporate finance business line.

The liability to keep total capital is calculated as the three-year average of the simple total of the legal capital stock liability calculated for each year in each of the business line. Although it was mentioned that in any year, in any business line, it would eliminate the positive capital amounts in other business line by reason of negative capital amounts arising out of negative gross income, the national authority stated that the negative capital amount in a business line should be clarified, without any restrictions, with the positive capital amounts in the other businesses. Nevertheless, if the total liability to keep capital stock in a certain year for all business line is negative, the value that needs to be written to the numerator part of the fraction for that year shall be zero. However, as is the case in the Basic Indicator Approach, in Standardized Approach, if the negative gross income distorts the Primary Structural Block capital amount of a bank, supervisory authorities shall evaluate implementation of suitable measures within the scope of Secondary Structural Block (www.bddk.org.tr/WebSitesi/turkce/Basel-II/1249Basel%20II%20Cevirisi-14102005-16_19.pdf, 2009).

The total liability to keep capital stock according to the standardized approach is as follows;

$$Capital_{SA} = \{_{years} 1\text{-}3 \max [(BG_{1-8} \times \beta_{1-8}), 0]\} / 3$$

$Capital_{SA}$: Liability to keep capital stock according to Standardized Approach

BG_{1-8}: For each of the business line, annual gross income in a certain year

β_{1-8}: For each of the eight business line, a fixed rate that connects the required capital level to gross income level and that is specified by the Committee.

Since the beta coefficients have changed up to the stage they got their final shape, Alternative Standardized Approach (ASA) which is a type of the Standardized approach has emerged. Alternative Standard Approach is similar to the Standardized approach, and the only difference between them is that in ASA approach, 3.5% of the total receivables in the assets for retail banking and corporate banking fields of activity is used instead of the gross income. In the second option that is evaluated under the ASA approach, for retail banking and corporate banking business line, 3.5% of the total receivables in the assets for these business lines are multiplied by 15%, whereas the total gross income for the other business line is multiplied by 18% (www.bddk.org.tr/WebSitesi/turkce/Basel-II/1254QIS-TR.pdf, 2009).

2.3.4.3 Advanced Measurement Approach

According to Teker (2006) advanced measurement approach is a more complex and risk responsive method. Calculation of operational risk capital provisions with this approach depends on internal measurement systems of the bank. The banks will be able to calculate capital provisions for the operational risk with the condition to comply with the quantitative and qualitative criteria specified by BIS by taking as basis the data to be obtained from the internal measurement systems.

AMA is a method for banks to develop their own model for assessing the regulatory capital that covers their yearly operational risk exposure within a confidence interval of 99.9 (this exposure is operational value at risk, OpVaR). A statistical model is used in insurance sector which is derived from eligible variants of AMA. This model is often referred to the loss distribution approach (LDA) which has become a standard in the industry over the last few years. (www.sciencedirect.com.library.bilgi.edu.tr/science?_ob=ArticleListURL&_method=list&_ArticleListID=1368171579&_sort=r&view=c&_acct=C000

052709&_version=1&_urlVersion=0&_userid=1437276&md5=150c97e16ae0be8c816942e8865d09de, 2010).

The committee has aimed that the banks should set aside lower capital provisions by using the advanced measured methods. However in this method a lower limit has not been specified for the risk provisions. In other words, the banks will set aside capital provisions the extent they can measure their data. Therefore, advanced measurement approaches are known as a method of encouragement. However, difficulties in finding sufficient and high quality data are the biggest problem related to this approach.

The fundamental belief in the banking sector is that the Basic Indicator Approach and the Standardized Approach cannot be connected to significant indicators and therefore operational risk capital requirement that will be calculated by using these methods will not be realistic. Therefore, the status in the banking sector is that international banks develop their own measurement risk methods and prefer calculating the capital requirement in respect of operational risks by using this method (Teker, 2006).

The positive side of these methods is that they allow for further development in quantifying the operational risks which is a newly developing field, and the negative side is that they encumber the supervisory authorities with more burdens of duties by entrusting those important duties and responsibilities in allowing use of these methods. The Committee gives the supervisory authorities the liability to make the reliability of the advanced measurement approaches subject to detailed assessment within the scope of 2nd Structural Block (www.tkgm.gov.tr/turkce/dosyalar/diger%5Cicerikdetaydh337.pdf, 2009).

Advanced measurement approaches are mainly formed up of four different approaches. These are;

• Internal Measurement Approach

• Loss Distribution Approach

• Scorecard Approach

• Scenario Analysis Approach

Internal Measurement Approach: This approach requires that the banks form their loss data bases and information and reporting channels that will keep the said data base up to date. In this manner, statistical data that will be acquired out of the loss data base shall be used to estimate the highest loss amount that the bank may sustain within a specific period of time by reason of operational risks at a certain security level. This approach generally is based upon a framework in which the bank's activities are separated to business lines and operational risk events. Within this framework, a separate expected loss is calculated for each business line and event type combination. Expected losses are calculated by way of estimating loss probability (PE), loss event (LGE) and exposure indicator (EI).

Operational risks are classified on the basis of event types and bank's fields of activity, a different risk parameter are determined for each business line and for each event type. The capital that will be reserved for each business line is the value to be reached by multiplying the relevant parameter by the probability of occurrence of such risk, its severity, and the volume of the bank in that business line (www.riskcenter.com.tr/operasyonelrisk/operasyonelfiles/veritaban.pdf, 2009).

Capital provisions are set aside in the form of a certain percentage of the expected losses.

Capital Provisions = Expected Loss x factor specified by the regulatory authority (gamma)

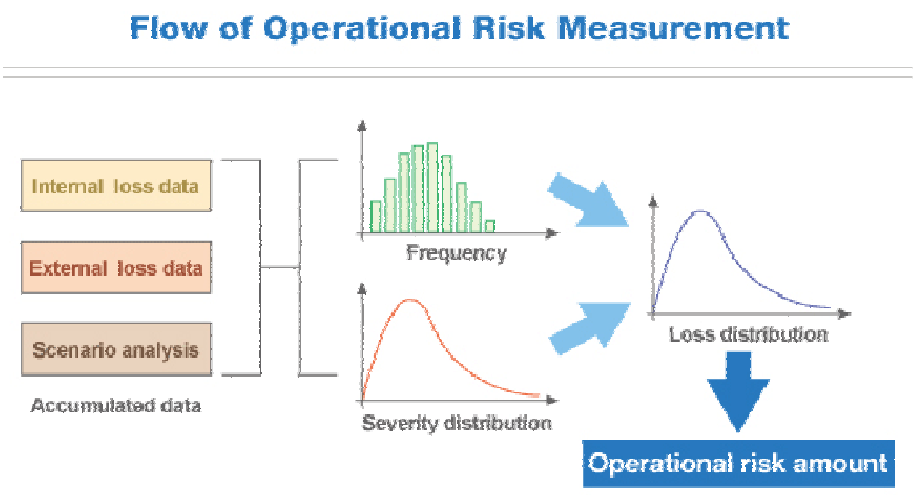
• This approach takes into consideration “event types” as different from the Standardized Approach.

• Risk indicator of the bank for each business line /type of event (EI) should provide the loss probability (PE) and actualized loss event (LGE) data

• Expected Loss (EL) = EI x PE x LGE

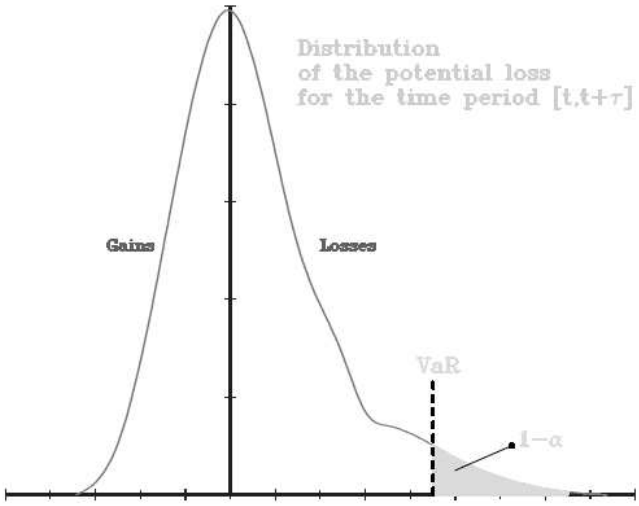
• Capital = EL x Gamma factor

Figure 2.5: Advanced Measurement Approach
(www.fintec.co.jp/english/business/management/others.html, 2009)



Loss Distribution Approach: In this method, distribution of the operational risk loss amount is estimated within a certain time interval. Total capital provisions are specified by taking the totals of “value at operational risk” (OPVaR). The following figure indicates loss distribution:

Figure 2.6: Loss Distribution and Value at Risk (www.thierry-roncalli.com/download/lda.pdf, 2009)



It uses the loss data base within the bank and measures the probability of each risk to occur within the next year and in case of occurrence of the risk the severity thereof, and by using various statistics, it calculates the ORVaR. In other words, the bank estimates the probable distributions of the operational risk losses that may occur within a certain period for each business line/event type. We may list the stages of this method as follows;

• Gathering of internal and external data to allow their utilization,

• Defining the frequency and severity levels separately on the basis of key risk fields in all fields of activity,

• Forming loss distribution curve by using various techniques,

• Calculating the capital based on the results (www.riskcenter.com.tr/operasyonelrisk/operasyonelfiles/veritaban.pdf, 2009).

Scorecard Approach: In the scorecard approach, the risks in the relevant activity fields are assessed by the field manager with the help of a scorecard and then are converted into capital. The superiority of this method is that it does not depend upon only historical data. Historical data

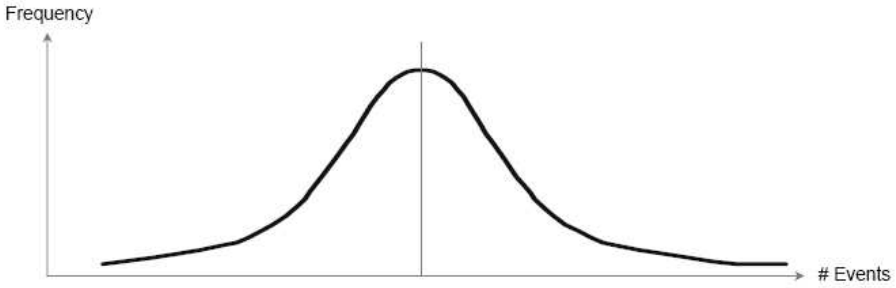
are used in confirming the results of the scorecard approach (www.tkgm.gov.tr/turkce/dosyalar/diger%5Cicerikdetaydh338.doc, 2009).

In this approach, the banks determine the beginning level of operational risk capital by taking as basis the whole of the bank or the level of field of activity and change this amount in time based on the scorecard. Scorecard tries to determine the importance of risk profiles and risk control environment in various fields of activity. This approach aims to bring a viewpoint that is aimed at the future for capital calculations. In this manner, developments surrounding risk control that will mitigate the frequency and severity of future operational risk damages are reflected. Scorecard might be based on actual risk measurements. However, it defines the indicators representing certain risk types in fields of activity of operation units.

Scenario Analysis Approach: It is an approach by which the banks measure their risks by creating scenarios for themselves. Banks classify the risk profiles that they determine by way of question tests, by resorting to the opinions of experts, by taking into consideration the complaints and similar methods and put them into writing in the form of scenarios. Later on, they assess these scenarios in terms of potential frequency and potential severity as shown in the following figure

Figure 2.7: Scenario Analysis Approach

(www.boj.or.jp/en/type/release/zuiji_new/data/fsc0608be7.pdf, 2009)



The Number of Events

and

The Impact/Severity of Events

The data obtained as a result of evaluation of the scenarios are analyzed by way of statistical techniques. Parameters are determined by using the analyzed data and risk models are formulated using such parameters. Later on, for potential losses that are obtained from these risk models, the capital that will be set aside within a certain security limit, are specified by using statistical techniques.

Advanced measurement approach based on scenarios combines the important parts that are necessary for a significant risk assessment. It increases perception of the risk. Empirical data and expert opinions are combined. This helps the organization to benefit from past experiences and to consider natural changes that occur during the dynamic business environment (www.riskcenter.com.tr/operasyonelrisk/operasyonelfiles/veritaban.pdf, 2009).

3. ROLE OF INTERNAL AUDIT FUNCTION IN BANKS ON OPERATIONAL RISK MANAGEMENT

3.1 Definition of Internal Audit

In the work of Güredin (2009) internal audit is defined as a type of audit in which financial and non-financial activities are reviewed and assessed.

Internal audit is an independent and objective control and consultancy activity that has been designed to add value to the activities of an organization and to develop these activities.

3.2 Importance and Purposes of Internal Audit in Banks

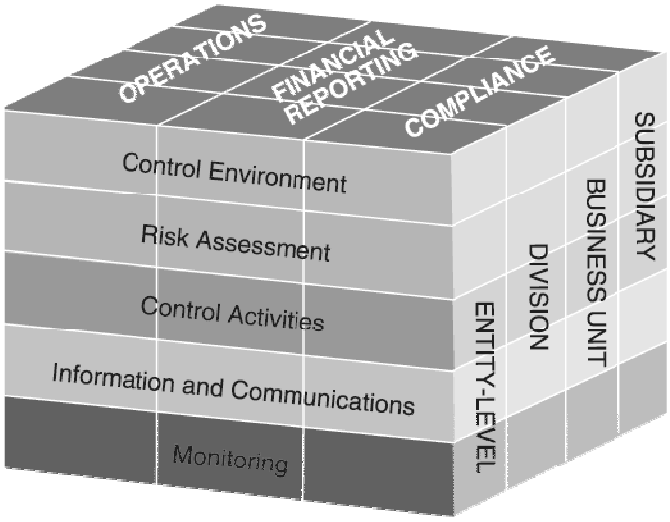
Internal audit is a function which involves bank's board of directors, high level management and other bank personnel. It is not a policy or practice pertaining to a certain period of time, but is an activity that shows continuity at all levels of the bank. According to BRSA regulations, Turkish Bank's board of directors and high level management are responsible for forming an intra-bank culture, maintaining and monitoring its efficiency. However, it is necessary that all the bank personnel also participate in the audit function. The purposes of internal audit can be listed as follows (www.oenb.at/en/img/bcbs92_tcm16-15498.pdf, 2009);

- Efficiency and effectiveness of activities, (performance objectives)
- Reliability, integrity and timing of financial and administrative information (objectives in respect of information systems)
- Compliance with existing laws and regulations.

These three objectives are also main component of COSO dimensional matrix as shown in the following figure:

Figure 3.1: COSO Dimensional Matrix

(www.glovia.com/html/news/newsletter/02_04/feature.asp, 2009)



Objectives of internal audit in respect of performance are effective and efficient use of bank resources and prevention of possible damages. With the internal audit function, it is aimed to ensure that all the bank's personnel keep the bank's interest superior to all kinds of personal and other interests and work effectively to realize the bank's objectives. On the other hand, it is aimed to provide bank's decision-making organs reliable and accurate information and reports. At the same time, it is aimed that the year-end balance-sheet data and other financial figures and the reports given to shareholders, supervisory authorities and other third parties are accurate and reliable (www.oenb.at/en/img/bcbs92_tcm16-15498.pdf, 2009).

The aim is to ensure that all the activities of the bank comply with the relevant legal arrangements, the standards specified by supervisory

authorities and the policies and methods of the bank. In order to protect the reputation of the bank, it is necessary to comply with the said principles.

3.3 Basic Elements of Internal Audit System in Turkish Banks

The scope of internal audit which is a function which first aimed to minimize the probability of fraudulent acts, abuse of duty, and fault developed in time and it turned into a system that can reveal all kinds of risks that can be encountered by a bank. Internal audit system is significant in order for a bank to realize its objectives and to maintain its activities. Internal audit system is comprised of five basic elements, which are associated with each other.

a. Supervisory activities of the bank management and intra-corporation audit culture

b. Risk recognition and assessment

c. Audit activities and functional division

d. Information Access system and intra-corporation communication

e. Monitoring activities and correction of faults in the internal audit system

Problems that are observed in banks that have sustained considerable amounts of damage can be listed within the scope of these elements. Realization of objectives concerning performance of the bank's internal audit function, information systems and their compliance with legal and other arrangements depends upon effective functioning of the five elements listed above.

3.4 Internal Audit Function in Banks and the Framework of Operational Risk Management

Banks in which operational risk management is the most effective are the banks that have the highest ethical conduct standards in both the branches and also the head office departments (www.emeraldinsight.com/Insight/viewContentItem.do;jsessionid=5E7233D0E4B2A7CE9DDD381C6509F708?contentType=Article&hdAction=lnkhtml&contentId=1603667, 2009).

Internal operational risk culture of a bank is comprised of individual and corporate values, attitudes, competencies and conducts that help the bank to fulfill its liabilities and the style of Operational Risk Management.

Board of Directors and top management are responsible for creating an organizational culture that will help operational risks to be effectively managed and operational controls to be made in an appropriate manner.

Basel Committee has determined how these objectives shall be realized in the first three principles of its study "Sound Practices". These can be summarized as follows (www.bis.org/publ/bcbs91.pdf, 2009);

Organizational Structure: The Board of Directors is responsible for establishing a management structure that will help to implement an effective Operational Risk Management framework for the bank. Internal audit function which is an important part of this process shall review the following matters;

• Whether the Operational Risk Management has the qualified personnel who have the necessary information, has sufficient technical possibilities and has access for the required resources.

• That the employees who are responsible for managing the operational risks in all the business units of the bank are determined

• That segregation of duties among operational risk control functions, business lines and support functions are made

• That Operational Risk Committee is established and the duties and responsibilities of the senior management are determined by such committee.

• Set up of an effective communication network between operational risk management and business units.

Responsibilities of the Board of Directors and the Top Management: One of the most important factors in adapting an effective operational risk framework to the bank successfully and implementing it is the effective involvement of the Board of Directors and Senior Management in this process. Within this context, the internal audit function shall verify the following matters;

• Approval should be taken from the Board of Directors for the Operational Risk Management Framework that will be applied in the bank. In this framework, the operational risk should be accurately defined; it should cover the risk appetite of the bank and its tolerance of operational risks and should include the policies to be implemented for management of the operational risks.

• Senior management is responsible for implementing the said Operational Risk Framework, and for developing the policies, processes and procedures in respect of management of the operational risks.

Manual of Policies, Processes and Procedures: Senior Management should detail the Operational Risk Framework and develop special policies, processes and procedures. These should be applicable and should be verified by discussing with the business units. Internal auditors should check the existence of these manuals, and review the contents and implementation by the management. In addition, internal auditors will

review whether these manuals are being appropriately updated and are being shared with the bank's employees at all levels (www.tkgm.gov.tr/turkce/dosyalar/diger%5Cicerikdetaydh338.doc, 2009).

3.4.1 Establishment of Operational Risks

The New Capital Accord requires that operational risks are determined continuously, systematically and fully (Sheen, 2005).

For this reason internal audit function should:

- confirm whether there is a special process for determining the operational risks
- confirm whether the operational risk function is able to determine weak points
- ensure that the process is fully put in writing
- review whether the control procedure developed by the operational risk function reflects the objectives and rules of the organization

In order to realize the above, the internal auditor should:

- analyze the quality of the documents prepared in relation to determination of the operational risks
- confirm that the process is consistent and accurate in terms of time and form

Internal and external factors that adversely affect the bank to each its objectives must be taken into consideration. Therefore, the internal auditor should take into consideration the following internal risk factors;

- Inadequate organization structures that do not support distribution of functions or monitoring and analysis of the activities in the bank

• Non-existence of a documentation in which the processes and procedures concerning bank's activities are explained

• Non-existence of a documentation that defines the management environments in different fields

• Non-existence of a corporate management that influences decision-making processes

• Non-existence of ethical rules that regulate the performance of the firm

• Deficiencies in the automation of the main processes

• Deficiencies in the personnel election and training processes

• Non-existence of mechanisms that will help effective monitoring of operations and processes (www.tkgm.gov.tr/turkce/dosyalar/diger%5Cicerikdetaydh338.doc, 2009).

Internal auditor should take into consideration the following external risk factors:

• Whether the used technology is up to date

• Adoption of procedures to the new legal framework or monitoring of practices

• Adaptation to new markets, products or activities

• New fraudulent acts or misuse of authority

• New activities containing high risk

3.4.2 Assessment of Operational Risks

Banks must assess the operational risks which are involved in all the products, activities, processes and systems. Effective risk assessment should be made qualitatively and quantitatively.

3.4.2.1 Qualitative Assessment

Internal auditors must determine models to establish whether or not there is an accurate and sufficient assessment model. In many of the cases, this model must use the information that will be received from the business lines and the loss event types to be determined by New Capital Accord.

Certain cases that must be reviewed by internal audit have been specified below (www.oenb.at/en/img/bcbs92_tcm16-15498.pdf, 2009).

- Design of the model used for assessment of the operational risks of the bank
- Appointment of operational risk managers responsible for defining and assessing the operational risks for all organizational fields
- Participation of the operational risk unit in committees were new activities, products, processes and systems are approved
- Involvement of all groups and business lines in the function assessment model
- Relationship between the bank's organizational fields and the business lines specified by New Capital Accord
- Sufficiency of the operational risk processes realized by branches
- Sufficiency of the approaches used in transfer of risks from support departments to business areas of the firm
- Existence of a procedure to be used for updating organizational data in case of a structural change

• Regular reporting between Operational Risk Department and the management

• Existence of detailed documentation that can be understood by third persons in respect of operational risk models and the employed tools

The other factors that need to be taken into consideration by the internal audit function while determining its procedures have been listed below.

Data Gathering Process: Ensuring reliability of the results received from the assessment model

Internal Validation: Internal Validation processes assess the performance of the internal models. Therefore, they must assess the quality of the results obtained from the tools used by internal auditors (www.tkgm.gov.tr/turkce/dosyalar/diger%5Cicerikdetaydh303.pdf, 2009).

Qualitative assessment parameters: Review of the correctness and documentation of the parameters employed in the assessment model.

3.4.2.2 Quantitative Assessment

Basic two quantitative factors used in operational risk management other than internal control factors, scenario analysis and external data are analysis of risk indicators and loss events. Internal auditors should prepare the procedures by reviewing these factors. It should be remembered that these factors come together with the qualitative factors in the general operational risk structure of the firm.

3.4.2.2.1 Risk Indicators (KRI)

According to Marshal (2001) risk indicators are statistics and/or matrices that demonstrate the performances of the processes of the company which may be exposed to risks.

These indicators warn the banks against changes that will affect keeping of planned budget in limit.

The following matter should be taken into consideration at the time of determining the objectives of the review of these risk indicators and the audit procedures.

Existence of the Quantitative Measurement System: Internal auditors must verify the existence of a quantitative measurement system in respect of operational risks. This system must complement the results of qualitative assessments. Furthermore, they must conform to the operational risk management process of the company. In this manner, internal auditors must verify the existence of the necessary tools for defining, calculating and monitoring the indicators.

Power of estimation of the system: It is necessary to measure the quality of the data used in the calculations by the internal auditor. Nevertheless, the internal auditor should also assess the appropriateness of the historic data loss series for statistical calculations.

Monitoring of Indicators: Internal auditors must inspect whether the indicators are regularly reviewed, monitored and analyzed by the operational risk function.

Reporting the results to the relevant departments and to senior management: It is necessary to make regular reporting so that the necessary information within the company is shared by the relevant departments and senior management. To this effect, internal auditors must review the timing accuracy and usefulness of the reporting

(www.emeraldinsight.com/Insight/viewContentItem.do;jsessionid=5E7233D0E4B2A7CE9DDD381C6509F708?contentType=Article&hdAction=lnkhtml&contentId=1603667, 2009).

3.4.2.2.2 Analysis of Operational Loss Events

Operational risk loss events are caused by one or more operational risk types. They usually cause losses, but later on, losses may be revealed, mitigated or eliminated using various mechanisms. Some of these mechanisms are internal controls, management, insurance and civil court cases. Firms generally have the tools for defining, assessing, inspecting the operational risks and mitigating the cases.

Internal auditors should prepare their audit plans, objectives and procedures by taking the following into consideration.

Existence of a reliable model for loss data collection: This model provides information on the risks arising from the business line and the risk types specified in the New Capital Accord.

Loss data collection infrastructure: Banks must have suitable and strong infrastructures in order to carefully and systematically monitor and record events causing operational loss (www.riskcenter.com.tr/operasyonelrisk/operasyonelfiles/veritaban.pdf, 2009).

Within this context, internal auditors should prepare their procedures in such manner that they check the existence of automatic capture of events and compliance of the degree of automation with the management responsible for reporting and reviewing the operational losses.

For control of the non-automotized events, internal auditor must review the manual data capture procedures.

For the existence of a suitable automatic capture of data infrastructure, it is necessary to review the technical characteristics of the employed tools used for automatic data capture, review the written instructions for the personnel recording the data and to review the control mechanisms that provide accuracy of the recorded data.

Reporting of loss events: Internal auditors must verify the existence of the procedures that help recording of all events (www.bulentsenver.com/Kultur/pdf/riskyonetimiprensipleri.pdf, 2009).

Validation of results: Internal auditors must be sure that the results match with the actual status of the company.

Action plans for development: Internal auditors must verify that necessary actions for development of the risk control are taken after due review of the results.

Reporting of the results to the relevant departments and senior management: Internal auditor must review the timing of the reporting and whether it contains all the necessary information for operational risk management process. The following information must absolutely exist.

- Summary of the losses according to risk types and business lines
- Global evaluation according to business lines and risk event types
- In case the losses are intensified in a region or in a certain type of case reasons thereof and the action plans to be taken
- Current status of the minimum capital requirement and evaluation of the past
- Status in the sector

Reporting the results to the market: Internal auditors must inspect whether the information regarding operational loss level conveyed to the

market in the annual report conform to the risk profile and the conditions of New capital Accord.

3.5 Operational Risk Mitigation

Implementation of the operational risk assessment system should be made so as to allow mitigation of the specified risks, in a manner that suits the risk thresholds specified under the firm's strategy and in line with the objectives specified by the operational risk function (www.tkgm.gov.tr/turkce/dosyalar/diger%5Cicerikdetaydh274.pdf, 2009).

Internal audit function must prepare its procedures by taking the following into consideration.

Contents and presentation of the reporting to the relevant departments and senior management: Internal auditor should check whether the reports are sent on time and to the persons who are responsible for assessing the reports in the relevant fields. The reports should contain the obtained results and the comments of the evaluators before submission to the senior management. The information in the reports that have been prepared should be included in the relevant decision making processes.

Formation of action plans: During the assessment process in-depth analysis of the results should be made. Action plans must be prepared so as to mitigate the operational risks that are higher than the acceptable level or those operational risks for which such action plans have been required. Action plans must be prepared with the participation of operational risk management authorities and authorities of the different fields of the organization and unanimously. Internal auditor must verify the existence of action plans, establishment of priorities in practice and level of development(www.emeraldinsight.com/Insight/viewContentItem.do;jsessionid=5E7233D0E4B2A7CE9DDD381C6509F708?contentType=Article&hdAction=lnkhtml&contentId=1603667, 2009).

Monitoring of Action Plans: Tools must be prepared so as to ensure that actions plans are effectively implemented by the operational risk function. Internal auditors must verify the existence of these types of tools. It is necessary to inspect whether an implementation calendar for the action plan is in place and the operational risk function follows up implementation of the plan.

3.6 Monitoring and Reporting of Operational Risks

Internal auditors must investigate the existence of an external reporting process that gives information to third parties (external auditors, markets, agencies, relevant authorities, etc) regarding the exposed operational risks, rules and procedures used for operational risk management, actions taken by the company for realizing the operational risk objectives and the data used. All these efforts that try to make operational risk management systematic can be used for the decision making mechanism and if they do not provide full information, it is meaningless. However, it is also very important that this information reached the relevant places and is considered by the management.

Internal auditors must analyze different reports and the below-specified main characteristics.

- Purpose, ensuring that the information in the reports make it possible to determine the problematic areas and the actions taken to correct them
- Distribution, ensuring that the information is sent to senior management and to the responsible persons in the relevant departments and that the information is received by such persons
- The time intervals at which the reports are distributed and whether the information in them is up to date
- Source of information

• Who is responsible for developing and checking the information

Furthermore, in order that this information can be used by the internal auditors and to allow the management to monitor them, their efficiency must be controlled.

3.7 Methodology of Capital Calculation

Basel Committee has constituted the foundations for calculation of the capital to be set aside for operational risks. The different types of approaches have been determined, depending on complexities. The qualitative and quantitative rules that the company must comply with are determined according to the selected methodology (www.makalem.com/Search/ArticleDetails.asp?nARTICLE_id=1294, 2009).

A bank should have the tools of Loss Database, Key Operational Risk Indicators, Scenario Analysis, Risk Control Self Assessment in order to calculate accurately the capital for operational risks. In this respect, Bank's Board of Directors should support Operational Risk Management in terms of budget and human resources.

For this reason, internal auditors must be able to review the validation of the methodologies and the requirements of practice and they must be able to contribute.

Within this context, the level of information that the internal auditors must have are determined according to the methodology that is used. While in the basic indicator approach, the role of audit is to review the compliance with the qualitative criteria, in the advanced measurement approach method it is necessary to understand statistical and mathematical techniques that are used, ad to have in-depth knowledge about the organization and the financial sector in general.

Independent from the selected methodology, internal auditor must inspect the compliance of different procedures used in operational risk management with the conditions of capital methodology that has been implemented.

During this review, the internal auditor must take into consideration the following:

- Existence of a function responsible for determining the requirements of operational risk capital
- Automation of the processes and level of implementation of controls
- Existence of an audit process that controls the accuracy of the calculations
- Determining threshold and existence of cautionary signal in case the thresholds are exceeded
- Reporting work flows in which all the relevant information is submitted to the senior management with sufficient details
- Documentation of the information used for calculation

3.7.1 Basic Indicator Approach

The auditors must be sure that selection of this method instead of review of the capital calculation is not inappropriate for the operational risk management of the company by reason of its simplicity.

3.7.2 Standardized Approach

Auditors must verify the accuracy of the documented rules, existence of the criteria of distribution of the gross income to eight business

lines and the accuracy of the calculations. The following must be included in some of these verifications.

Distribution of all the activities of the company to business lines detailed in the New Capital Accord criteria by using objective criteria. This distribution must also conform to the methodologies used for credit risk and market risk (www.bddk.org.tr/WebSitesi/turkce/Basel-II/1249Basel%20II%20Cevirisi-14102005-16_19.pdf, 2009).

- Providing a consolidated approach towards management procedures and fields that are concerned with the management of other risks (compliance, credit, market etc.) and ensuring coordination in respect of distribution of activities to business lines

- Taking into consideration the operational risks, new products and new activities, designs, analyses and approvals

- Review of the gross income of each activity distributed to the business channels

- Accounting structure according to business lines

- Finding appropriate documentation in respect of approach of distribution of operational losses to business lines

- Documented official rules must be approved by the senior management by taking into consideration whether the income has been distributed to business lines and taking into consideration capital requirements.

3.7.3 Advanced Measurement Approach

In order that the conditions required by regulatory authorities for this complex method are implemented in an effective manner, the bank needs to pass through a very strong preparatory process. When a bank

decides to implement advanced measurement approach, it is necessary to be involved in the internal audit function process and to control and analyze the following dimensions.

- Existence of a global plan by which the new functions that need to be assumed by the operational risk department in order to implement and monitor the necessary models can be reviewed and monitored.

- Existence of an operational events manual accessible to all employees

- Formation and arrangement of plans and processes that will allow all the employees to determine and analyze the operational events

- Preparation of the necessary processes for determining and gathering operational data losses

- Implementation of the necessary processes for analyzing and determining the bills and accounting entries which are the parts of the process of determining operational losses

- Existence of operational loss database that will allow operational risk function to manage the information easily

- Establishment of the flow of reporting to be made to the senior management and to relevant departments

- Existence of the audit processes that will validate the achieved performance(www.emeraldinsight.com/Insight/viewContentItem.do;jsessionid=5E7233D0E4B2A7CE9DDD381C6509F708?contentType=Article&hdAction=lnkhtml&contentId=1603667, 2009).

One of the most important issued that need to be considered at the time of beginning to implement advanced measurement approach is requirement for historical series (minimum 3 years, preferably 5 years and

more) of the loss data to be used in the statistical models and capital model (Bank of Spain, 2006).

Therefore, internal auditors should focus on the following matters in relation to collection of operational loss data.

- Existence of databases containing the information necessary for defining the loss events
- Relationship between the collected operational losses and accounting records
- Formation of approaches for distribution of the operational losses to business lines
- Existence of the necessary procedures to consolidate the information related to many losses arising out of a main case
- Ensuring that the used historical series provides that the event it resulted from is not lost, even if the loss is wholly covered, and allows determining of the events occurring on a certain date
- Development of the analysis of the correlation of historical series of operational losses with the internal and external factors that influence operational risks
- Making and recording frequency and severity curve analyses of operational events

4. ABC BANK'S INTERNAL AUDIT FUNCTION ROLE IN OPERATIONAL RISK MANAGEMENT

4.1 Purpose of the Study

The objective of this study is to provide a global perspective of the operational risk management framework from an internal audit viewpoint by reviewing ABC Bank's applications.

4.2 Methodology of the Study

This study describes the responsibilities and activities of the internal audit department of ABC Bank in reviewing the operational risk framework.

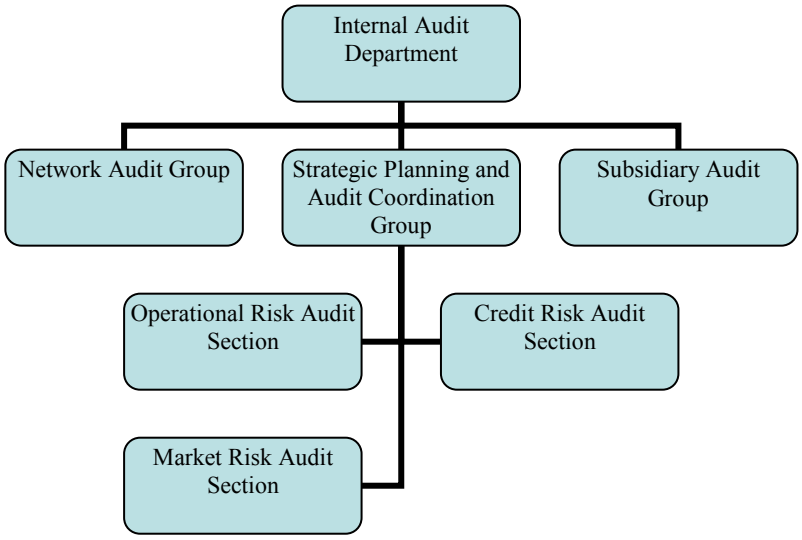
4.3 Review of ABC Bank's Internal Audit Department Activities in Operational Risk Management

ABC Bank is a private and commercial bank which is active for long years and which is one the big 10 banks in Turkey based on asset size. It has above 5 subsidiaries within the country and above one subsidiary in abroad it gives all the core banking goods and services with above 500 branches, above 1000 ATMs and above 10.000 personnels. When the shareholding structure of the bank is reviewed, above 5% is connected to a foreign finance group and the rest is connected to a Turkish finance group.

4.3.1 Organizational Structure of ABC Bank's Internal Audit Department

Internal Audit Management of ABC Bank has been continuing its activities since the date of its incorporation. It continues its Internal Audit Management activities under 3 groups as shown in the following table:

Table 4.1: Organizational Structure of ABC Bank's Internal Audit Department



Branch Audit Group: it conducts the activities of auditing branches within and outside the country.

Strategic Planning and Audit Coordination Group: It conducts the activities of auditing the General Management units. It is made up of three sub departments;

• **Credit Risk Audit Department:** It conducts the auditing of units which constitute credit risk in Head Office.

• **Operational Risk Audit Department:** It conducts the auditing of units which constitute operational risks in Head Office.

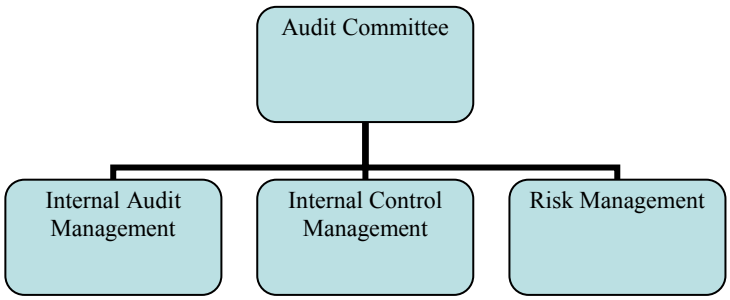
• **Market Risk Audit Department:** It conducts the auditing of units which constitute market risk in Head Office.

Subsidiary Audit Group: It conducts the auditing of units which constitute operational risk and credit risk in ABC Bank's subsidiaries.

4.3.2 Role of Internal Audit Management in the Organizational Structure of the Bank

Internal Audit Management in ABC Bank is within the Audit Committee. Audit Committee reports to the Board of Directors. Reporting of the Internal Audit Management to Audit Committee allows it to conduct its activities independently. The Organizational Chart can be found below;

Table 4.2: Organizational Structure of Audit Committee in ABC Bank



As it can be seen above, Internal Audit Management and Risk Management are under the same framework of Discipline Committee.

4.3.3 Organizational Structure of Operational Risk Management Unit of ABC Bank

In ABC Bank, Risk Management is an independent department which directly reports to Board of Director. It is comprised of the units of

Credit Risk Management, Operational Risk Management and Market Risk Management. Risk Management, as can be seen in the above chart, belongs to the Audit Committee as Internal Audit and Internal Control Managements.

4.3.4 Job Descriptions of Operational Risk Management

The duties of Operational Risk Management are to determine the operational risk policy of ABC Bank, to determine guiding principles for forming methods to determine, assess, manage, measure and monitor the risks, to develop, implement risk measurement and monitoring models (method, metric and analysis models) and to calculate the operational risk capital requirements.

4.3.5 Activities Performed by Internal Audit Function within the Framework of Operational Risk Management

Annual Audit: Internal Audit Management conducts ordinary audit for once every year in the Operational Risk Management department. This audit is realized by the Operational Risk Audit Department under the Internal Audit Management. The auditors which realize the audit are auditors who have sufficient knowledge on operational risk management. These audit activities are realized regarding the efficiency and efficacy of operational works in the department, compliance of the responsibilities conducted by the department with legal regulations and effect of the activities realized by the department on the financial figures. In the audits, the following matters are reviewed specifically;

• **Operational Risk Data Base:** Primarily, it is reviewed whether the operational risk data base functions properly. It is questioned whether the systematic setups in the database conform to the Regulation on Operational Risk Management of ABC Bank. Through sampling methods, sample operational risk entries are selected. It is questioned whether the selected entries have been approved by the relevant management, whether

they have been entered into accounting records properly and whether there is any abuse.

• **Regulation on Operational Risk Management:** The regulation is reviewed by the auditors and it is questioned whether it is sufficient or not within the scope of current activities of ABC Bank and whether it is up to date or not. In addition, it is reviewed whether the necessary approvals have been obtained from the Board of Directors.

• **Operational Risk Assessment and Measurements:** It is questioned whether ABC Bank has established the operational risks accurately, whether it measured them accurately. In this interrogation, Operational Risk Entries are used. Furthermore, it is reviewed whether the risks assessed at the time of audit activities of the other departments have been entered to the Operational Risk Management System. Suggestions for improvement are made in regard with the deficiencies that are observed.

• **Calculation of Operational Risk Capital Requirement:** Calculation of Operational Risk Capital Requirement is done each year at the time of audit through re-performance method, that is, by repeating the calculation for purposes of verification.

• **Monitoring and Managing the Operational Risks:** In ordinary audit, it is questioned whether the operational risks of ABC Bank are being monitored correctly by the Operational Risk Management. It is questioned what kinds of preventative action plans are developed for the monitored operational risks, whether the developed action plans are applied to ABC Bank.

4.3.6 Monitoring Operational Risk Management Activities by Internal Audit Function

ABC Bank Internal Audit Management uses various tools to monitor the operational risks in the bank. It uses the results it has obtained

in the preparation of the annual audit plan. It also shares the results with the Operational Risk Management. The tools used by the Internal Audit Management for monitoring the operational risks in the bank have been explained below;

KORI (Key Operational Risk Indicator): Operational Risk Audit Department that works as connected to the Internal Audit Management, in all the ordinary audit it shall realized at the bank, reviews the key operational risk indicators that are prepared and followed up by Operational Risk Management in relation to the unit being audited. It investigates whether the KORIs actually cover the important operational risks in the relevant unit. It questions whether the information give by units to the Operational Risk Management regarding KORIs are accurate. In addition, it reviews the trend analyses made on a monthly basis by Operational Risk Management.

Scenario Analyses: Operational Risk Audit Department participates in the Scenario Analysis meetings organized by the Operational Risk Management and reports its views on the basis of the information it acquired during previous audits. As a result of the meeting, it investigates whether the corrective measures determined in relation to the scenario analysis have been fulfilled by the bank in due time. It evaluated the other matters that are shared by the relevant departments that attended the meeting and conducts special audit or review activities.

4.3.7 Critics of ABC Bank's Internal Audit Department Activities in Operational Risk Management

Operational Risk Data Base: Operational Risk Audit Section does not periodically review the operational risk entries. However, it should review the operational risk entries above the determined amount periodically. Internal audit should question whether the records have been approved by the relevant managements during its review. It should

investigate whether there are any abuses in relation to the entries and in addition review whether or not the records were put into accounts correctly. Besides, it should also specify on which subjects the operational risks are focused during these investigations by carrying out a trend analysis and it should organize the audit or investigation activities by moving from the results it has acquired.

Monthly Assessment Meetings: The Internal Audit Department does not periodically hold meeting with the Operational Risk Management for review realized operational risk in the Bank. Internal Audit Management should share the important operational risks it has determined within that month, whereas Operational Risk Management should share the important operational risks that entered into the operational risk data base and that were approved within that month, and important operational risks that it determined as a result of KORI analyses. Both management units should discuss the types of corrective measures that could be taken for these risks which have been assessed. Operational Risk Management should take the necessary action in order that the agreed corrective measures are implemented. Internal Audit Management should question whether these corrective measures which have been started to be implemented were completed in a timely manner.

CONCLUSION

Corporate governance became a highly important topic at the beginning of the twenty-first century. One of the reasons for becoming important is a number of large corporate scandals and failures. A strong internal control culture, which includes the internal audit function as a valuable source for internal and external risk information, is an important part of the corporate governance. Besides the internal audit and efficient operational risk management framework is important in order to improve and reinforce the internal controls of the banks.

Internal audit should have an important role in implementing systems for managing operational risk. The expectation from the internal audit function is not only supervising the procedures also creating value with recommendations which reinforces the operational risk management framework.

According to the result of this study, it is seen that internal audit departments of Turkish banks are not proactive in operational risk management activities. The main reason of this fact is that operational risk management is a new concept that Turkish banks have not fully adapted yet to their organization. In order to ensure that internal audit functions take an active part in operational risk management, banks first need to implement Basel II operational risk management principles clearly. On the other hand, internal audit departments of Turkish banks have traditional management style and strictly hierarchical business networks. This situation makes organizational and functional changes and adaptations of internal audit activities so difficult in terms of efficiency and effectiveness; also it interrupts to adopt proactive approach to operational risk management. As seen from this aspect, implementation of international standards of internal auditing, which describes internal audit department as a value added

function, ensure that internal audit functions adopt easily and perform effectively their roles in operational risk management.

This point of view will enable considering the management of the operational risk not only an obligation imposed by the authorities. An operational risk assessment and management system which is fully adapted to the corporate culture will give the banks the opportunity of differentiating in the sector. This differentiation will create a better image for the clients and also for the third parties.

REFERENCES

Active Akademi Araştırma Merkezi, "Bankalarda Performans ve Risk Yönetimi: Analitik Bir Çerçeve" *Active Dergisi* (October-November 2000):15: 3 May 2009 http://www.makalem.com/Search/ArticleDetails.asp?bWhere=true&nARTICLE_id=403

AKSEL, Kaan H., "Finansal Kurumlarda Operasyonel Riskin Ölçümü", *Activeline Gazetesi* 21 (December 2001) http://www.makalem.com/Search/ArticleDetails.asp?nAUTHOR_id=162&sResultType=BrowseAuthor&sLetter=&sAuthorText=Aksel,%20%20Kaan&nPage=2&nOrder=2&ALLRESULTS=1883,493,503,2068,4426,436,426,1110,457,478,1563,495,432,2545,1562,4437&Sayfa=2&nARTICLE_id=1110

ALKİN, Emre, SAVAŞ, Tuğrul and AKMAN, Vedat, *Bankalarda Risk Yönetimine Giriş* İstanbul: Çetin Matbaacılık (2001)

BABUŞCU, Şenol, *Basel II Düzenlemeleri Çerçevesinde Bankalarda Risk Yönetimi* İstanbul: Akademi Eğitim Yayıncılık (2005)

Bank of Spain, *"Implementation and validation of Basel II advanced approaches in Spain"* (2006)

BIS Basel, *"International Convergence of Capital Measurement and Capital Standards"* Basel Committee of Banking Supervision (June 2004): 27 September 2009 http://www.bis.org/publ/bcbs107.pdf?noframes=1

Basel Committee on Banking Supervision, *"Sound Practices for the management and supervision of operational risk"* (July 2002): 18 August 2009 http://www.bis.org/publ/bcbs91.pdf

Basel Committee on Banking Supervision, *"Internal Audit in Banks and the Supervisor's Relationship with Auditors: Survey"* (August 2002): 8 August 2009 http://www.oenb.at/en/img/bcbs92_tcm16-15498.pdf

Basel Committee on Banking Supervision, *"The matters to be considered related to the application of Basel II"* www.bddk.org.tr

BDDK, *"Bankaların İç Sistemleri Hakkında Yönetmelik*" (2006): 20 August 2009 http://www.bddk.org.tr/WebSitesi/turkce/Mevzuat/Bankacilik_Kanununa_Iliskin_Duzenlemeler/1678BANKALARIN%20%C4%B0%C3%87%20S%C4%B0STEMLER%C4%B0%20HAKKINDA%20Y%C3%96NETMEL%C4%B0K%20(2).pdf,

BDDK, *"Bankacılık Sektörü Risk Değerlendirme Raporu"* Bankacılık Düzenleme ve Denetleme Kurulu Araştırma Dairesi (June 2005): 15 August 2009 http://www.bddk.org.tr/WebSitesi/turkce/Raporlar/Bankacilik_Sektoru_Risk_Degerlendirme_Raporlari/302Risk_Raporu_haziran2005.pdf

BDDK, "Basel II Sayısal Etki Çalışması (QUIS-TR) Değerlendirme Raporu" Bankacılık Düzenleme ve Denetleme Kurulu Raporları (December 2004): 16 May 2009 http://www.bddk.org.tr/WebSitesi/turkce/Basel-II/1254QIS-TR.pdf

BDDK-BCBS, *"Sermaye Ölçümü Ve Sermaye Standartlarının Uluslararası Düzeyde Uyumlaştırılması (Yeni Basel Sermaye Uzlaşısı) Gözden Geçirilmiş Düzenleme)"* (June 2004): 14 May 2009

http://www.bddk.org.tr/WebSitesi/turkce/Basel-II/1249Basel%20II%20Cevirisi-14102005-16_19.pdf

BOYACIOĞLU, Melek Acar, "Operasyonel Risk ve Yönetimi", *Bankacılar Dergisi* 43 (2002): 27 October 2009 http://www.tkgm.gov.tr/turkce/dosyalar/diger%5Cicerikdetaydh338.doc

CAN, Evrim, *Operasyonel Risk ve Yönetimi* Ankara: Sermaye Piyasası Kurulu Yayınları (April 2003)

CANDAN, Hasan and ÖZÜN, Alper, *Bankalarda Risk Yönetimi ve Basel II* İstanbul: Türkiye İş Bankası Yayınları (March 2009)

CHAPELLE, CRAMA, HUBNER and PETERS, Ariane, Yves, Georges, Jean-Philippe. "Practical methods for measuring and managing operational risk in the financial sector: A clinical study" Journal of Banking and Finance. 32:1049-1061(2008) ScienceDirect. 25 May 2010 http://0-www.sciencedirect.com.library.bilgi.edu.tr/science?_ob=ArticleListURL&_method=list&_ArticleListID=1368171579&_sort=r&view=c&_acct=C000052709&_version=1&_urlVersion=0&_userid=1437276&md5=150c97e16ae0be8c816942e8865d09de

DENİZ, Sümer Özdemir, "Operasyonel Risk Yönetiminde Risk Azaltım Teknikleri" Risk *Yöneticileri Derneği Haber Bülteni* (September 2004) http://www.tkgm.gov.tr/turkce/dosyalar/diger%5Cicerikdetaydh274.pdf

FINLAY, Marc, *World-Wide Trends in Scenario Analysis* Bank of Japan, Operational Risk Scenario Analysis Workshop (2006): 3 November 2009 http://www.boj.or.jp/en/type/release/zuiji_new/data/fsc0608be7.pdf

FRACHOT A, GEORGES P.and RONCALLI T., *"Loss Distribution Approach for Operational Risk"* (2001): 8 October 2009 http://www.thierry-roncalli.com/download/lda.pdf

GÜREDİN, Ersin, *Denetim* İstanbul: Beta Yayıncılık (1999)

JARROW, Robert. "Operational Risk" Journal of Banking and Finance. 32: 870 – 879 (2008) ScienceDirect. 06 June 2010 http://0-www.sciencedirect.com.library.bilgi.edu.tr/science?_ob=ArticleListURL&_method=list&_ArticleListID=1368171579&_sort=r&view=c&_acct=C000052709&_version=1&_urlVersion=0&_userid=1437276&md5=150c97e16ae0be8c816942e8865d09de

LAVIADA, Ana Fernandez, "Internal Audit Function Role in Operational Risk Management" *Emerald* (2007): 15 May 2009 http://www.emeraldinsight.com/Insight/viewContentItem.do;jsessionid=5E7233D0E4B2A7CE9DDD381C6509F708?contentType=Article&hdAction=lnkhtml&contentId=1603667

MARSHAL, Christopher Lee, *Measuring and Managing Operational Risk in Financial Institutions: Tools, Techniques and other Resources* Singapore: John Wiley&Sons Inc. (2001)

MAZIBAŞ, Murat, *"Operasyonel Risk Ölçümü: Kayıp Dağılımları Modellemesi"* Bankacılık Düzenleme ve Denetleme Kurulu Araştırma Raporu (2005): 14 May 2009 http://www.tkgm.gov.tr/turkce/dosyalar/diger%5Cicerikdetaydh337.pdf

MAZIBAŞ, Murat, "Operasyonel Riske Basel Yaklaşımı: Risk Verilerine İlişkin Bir Değerlendirme" BDDK Araştırma Raporları (2005/2): 15 October 2009 http://www.bddk.org.tr/websitesi/turkce/Basel-II/1283MM_Opriskdata.pdf

Muziho-DL Financial Technology Co Ltd., *"Measure against Operational Risk"* 15 September 2009 http://www.fintec.co.jp/english/business/management/others.html

NUMANOĞLU, Mehtap "Global Ekonomik Gelişmeler ve Operasyonel Risk Yönetimi" *Türkiye Bankalar Birliği* (December 2008): 17 July 2009 http://www.tbb.org.tr/Dosyalar/Konferans_Sunumlari/224122008.pdf

POWER, Michael. "The Invention of Operational Risk" Review of International Political Economy. Vol:12 577-599(2005) JStor. 21 May 2010 http://0-www.jstor.org.library.bilgi.edu.tr/action/doBasicSearch?Query=operational+risk+management&wc=on

"Risk" *Büyük Türkçe Sözlük, Türk Dil Kurumu*, http://tdkterim.gov.tr/bts/?kategori=verilst&kelime=risk&ayn=tam

SAKA, Tamer, "Operasyonel Risk Ölçüm Tekniklerine Genel Bir Bakış" *Active Dergisi* 25 (July-August 2002): 27 August 2009 http://www.makalem.com/Search/ArticleDetails.asp?nARTICLE_id=1294

Sarbanes-Oxley Compliance Methodology for IT: 17 August 2009 http://www.glovia.com/html/news/newsletter/02_04/feature.asp

SEZGİN, Cüneyt and TÜZUN, Yasemin, "Dünyada ve Türkiye'de Piyasa Riski Yönetimi Uygulamaları" *Active Bankacılık ve Finans Dergisi* 17 (2001): 10 May 2009 http://www.makalem.com/Search/ArticleDetails.asp?nARTICLE_id=422

SHEEN, A., "Implementing the EU capital requirement directive – key operational risk elements" *Journal of Financial Regulation and Compliance* 13: 4 (2005)

SUPATGIAT, KENYON and HEUSLER, Chonawee, Chris, Lucas. "Cause-to-effect Operational Risk Quantification and Management." Risk Management. Vol.8 16-42 (Feb 2006) JStor. 20 May 2010 http://0-www.jstor.org.library.bilgi.edu.tr/action/doBasicSearch?Query=operational+risk+management&wc=on

SÜER, Gökçen, *Bankacılıkta Risk Yönetimi ve Türkiye Uygulamaları. Master Dissertation.* İstanbul: Marmara Üniversitesi Bankacılık ve Sigortacılık Enstitüsü (2002)

TBB Çalışma Grubu, "Risk Yönetimi Prensipleri" *Bankacılar Dergisi* 57 (2006): 15 October 2009 http://www.bulentsenver.com/Kultur/pdf/riskyonetimiprensipleri.pdf

TEKER, Dilek Leblebici, *Bankalarda Operasyonel Risk Yönetimi, Örnek Banka Uygulamalı* İstanbul: Literatür Yayıncılık (2006)

Türkiye Bankalar Birliği, *"Operasyonel Risk Veritabanı"* Risk Yönetim Sistemleri ve Uygulama Esasları Çalışma Grubu (April 2004): 8 November2009 http://www.riskcenter.com.tr/operasyonelrisk/operasyonelfiles/veritaban.pdf

YÜZBAŞIOĞLU, A. Nejat, "Risk Yönetimi ve Bankaların Denetimi" *Risk Yönetimi Konferansı* (16 Ocak 2003):13 March 2009 http://www.tkgm.gov.tr/turkce/dosyalar/diger%5Cicerikdetaydh303.pdf