İSTANBUL BİLGİ UNIVERSITY
INSTITUTE OF SOCIAL SCIENCES
FINANCIAL ECONOMICS MASTER'S DEGREE PROGRAM

RISK-BASED INTERNAL AUDIT AND DEVELOPING A RISK MATRIX FOR AUDIT PLANNING OF A BANK

Buşra Kevser SARUHAN
113621017

Asst. Prof. Derya ÜÇOĞLU

İSTANBUL
2017

Risk-Based Internal Audit and Developing a Risk Matrix for Audit Planning of a Bank

Risk Odaklı İç Denetim ve Bir Bankanın Denetim Planlaması için Risk Matrisinin Oluşturulması

Buşra Kevser SARUHAN
113621017

Dissertation Supervisor: Asst. Prof. Derya Üçoğlu .....
Jury Member: Asst. Prof. Faruk Z. Fırat .....
Jury Member: Assoc. Prof. Burcu Adiloğlu .....

Date of Approval : 13/10/2017

Total Number of Pages: 104

Keywords (Turkish)
1) Risk Odaklı İç Denetim
2) Risk Yönetimi
3) Kurumsal Risk Yönetimi
4) İç Denetim
5) Bankacılık

Keywords (English)
1) Risk-Based Internal Auditing
2) Risk Management
3) Enterprise Risk Management
4) Internal Auditing
5) Banking

Acknowledgement

I would like to thank to my supervisor Assistant Asst. Prof. Derya ÜÇOĞLU for her valuable contributions, comments and support.

TABLE OF CONTENTS

CHAPTER 2

INTERNAL AUDITING

CHAPTER 3

ENTERPRISE RISK MANAGEMENT ASSESSMENT

Abstract

Risk-based internal audit provides time and cost savings by concentrating on high risk areas determined as a result of risk assessment. Risk-based internal audit's success depends on effective risk assessment. Findings based on risk assessment provides an important source to internal auditors during audit.

In this study, the structure and development of the risk-based internal audit approach, benefits of having a risk-based audit approach, the structure of internal audit systems and the principles related to the effective audit in the banking sector were examined and an audit model was recommended for the risk-based audit of banking activities of branches.

It was also analyzed how these risks were evaluated and weighted considering the risk matrix suggested and fifteen risk factors affecting the branch activities of the banks. With the matrix formed according to risk-based internal audit approach; the areas with higher risk were chosen as the focal point and the efficient utilization of scarce audit resources was targeted.

Key Words: Risk-Based Internal Auditing, Risk Management, Enterprise Risk Management, Internal Auditing, Banking

Özet

Risk odaklı iç denetim; riskin değerlendirilmesi sonucunda belirlenen yüksek riskli alanları odak noktası seçerek, denetimde zaman ve maliyet tasarrufu sağlamaktadır. Risk odaklı iç denetimde başarının sağlanabilmesi, süreç içerisinde gerçekleştirilen etkin bir risk değerlendirme çalışmasıyla mümkün olabilmektedir. Riskin değerlendirilmesi sonucunda elde edilen risk bulguları, denetimin planlanması aşamasında, denetim görevini yürütecek iç denetçilere önemli bir dayanak sağlamaktadır.

Bu çalışmada, risk odaklı iç denetimin yapısı ve gelişimi, risk odaklı denetim anlayışına sahip olmanın faydaları, bankacılık sektöründe etkili denetime ilişkin esaslar ile iç denetim sistemlerinin yapısı incelenmiş ve bankalarda şube faaliyetlerinin risk odaklı denetim anlayışı yaklaşımıyla denetlenebilmesine yol gösterecek bir model önerisinde bulunulmuştur.

Önerilen risk matrisi ile bankaların şube faaliyetlerini etkileyen onbeş risk faktörü dikkate alınarak, bu risklerin değerlendirmelerinin ve ağırlıklandırmalarının nasıl yapılacağı analiz edilmiştir. Risk odaklı iç denetim yaklaşımı ile oluşurulan matrisle; daha riskli alanlar odak noktası seçilerek, sınırlı olan denetim kaynaklarının olabildiğince elverişli kullanılması hedeflenmiştir.

Anahtar Kelimeler: Risk Odaklı İç Denetim, Risk Yönetimi, Kurumsal Risk Yönetimi, İç Denetim, Bankacılık

INTRODUCTION

Banking operations; structurally integrated; contain many risks. Effective management of the risks related to banking operations is a guarantee for profitability and healthy growth.

The fast developments in the world have both caused expansion and diversification of risks that the banking sector has to face and manage in the international arena. All such experiences increased the need for internal audit. An effective internal audit system is required to carry out banking operations fully and securely.

Risk-based audit is an approach that should be implemented by banks in order to focus on identifying and managing the risks that the bank may face by allocating limited control resources to more risky areas.

Risk-based internal audit, by choosing a focal point for identifying high risk areas as a result of risk assessment, provides time and cost savings in supervision.

The aim of this study is to analyze the changes that took place over time in the audit approach, to explain the risk-based internal audit process in general terms and to evaluate the most important phases of this process, to explain in detail how the risks are determined and measured and how the risk-based internal audit plan is affected by this assessment as it is positioned within corporate risk management and as it is done by the internal auditor. With the risk matrix created as a result of risk assessment, risk levels of branch activities in the banking sector are determined and the audit process is planned according to the results. The audit activities and the necessary allocations are performed taking into account the current structure of audit resources.

CHAPTER 1

AN OVERVIEW OF THE AUDITING CONCEPT

1.1 AUDITING CONCEPT

Auditing concept, which can be described as review of activities of a person by another person, has a history back to all the way to 3000 BC. History shows that Mesopotamian kings authorized clerks to count stocks of royal grain silos to control officers based on archeological excavations. (Özoğlu et al., 2010, pp.29-30)

As stated in some sources, auditing activities dated to 3500 BC. For a long time, it was seen as a function to verify accounting calculations. (Sawyer & Dittenhofer, 2002, p.6)

Auditing can also be defined as comparing a person, organization, system, process, project, product or similar with a predefined standard or having them checked for compliance to the standards. (Ratliff and Reding, 2002, p.16)

In other words, auditing is a process for monitoring an organization, a person, an institution, a company, a system or a process within the framework of laws, by-laws, regulations and rules, in order to present their owners, shareholders, creditors, credit institutions, governmental administrative and economic units whether there are inconsistencies or deficiencies on various aspects, and whether the information presented in their financial statements are true and reliable. (Aksoy, 2006, p.47)

European Commission has also defined auditing as any examination performed to verify all aspects of a process/transaction, procedure or report. (Kurnaz and Çetinoğlu, 2010, p.11)

According to International Standard on Auditing (ISA) 200, “The purpose of an audit is to enhance the degree of confidence of intended users in the financial statements which is achieved by the expression of an opinion by the auditor on whether the financial statements are prepared, in all material respects, in accordance with an applicable financial reporting framework.” (ISA 200, para.3)

1.2 TYPES OF AUDIT

Audits may be classified on the basis of their purposes, on the basis of the organization and the status of auditor.

1.2.1 Audits Classified on the Basis of Purpose

Audits are generally grouped according to their purposes such as; operational audits, financial audits and compliance audits. Nevertheless, some subsections may be added to these classifications.

1.2.1.1 Operational Audits

Operational audits are systematic reviews to evaluate enterprises in terms of growth, profitability and improvement. Operational audits are performed to test feasibility and success of business goals based on these purposes. They present management possible drawbacks and problems that may be encountered while reaching business goals of an enterprise. (Kaval, 2003, p.25)

1.2.1.2 Financial Audits

Financial audits are conducted to determine whether the financial statements reflect the financial position and operational results of a company in accordance with generally accepted accounting principles and legal regulations. (Karanfiloğlu, 1999, p.30)

A financial audit evaluates whether an audited department's resources and liabilities comply with asset management and allocated budget allowances for that department. Problems identified are more than usual in an audit, a more detailed audit will be required on accounts for compliance with legislations. (Alptürk, 2008, p.22)

1.2.1.3 Compliance Audits

Compliance audits are used to determine whether implemented policies and rules are followed in organizations. For an auditor, parameters (rules followed by departments) are determined to evaluate departments' compliance and this process is called compliance audit. (Erdoğan, 2006, p.5)

In a compliance audit, processes/transactions performed by an enterprise are examined to ensure that they all comply with the laws, regulations, legislations and the enterprise's policies. (Yılmaz, 2004, p.22)

1.2.1.4 Information Systems and Banking Processes Audit

Information systems and banking processes audit is a process which reports information system management processes like software and hardware, processes related to banking activities and which presents opinions as a result of evaluating internal controls.

The main purpose of information systems and banking processes audit is to form an opinion about information systems, banking processes and also related internal controls in terms of efficiency, adequacy, consistency and compatibility. (Banking Regulation and Supervision Agency (BRSA), 2014, p.10) http://www.bddk.org.tr/WebSitesi/turkce/Mevzuat/Bankacilik_Kanununa_Iliskin_Duzenlemeler/9486bsd_yonetmeligi.pdf

1.2.2 Audits Classified on the Basis of Organization

Audits are not mandatory for all types of businesses. They are usually separated in two groups; audits which are performed as they are mandatory and audits which are performed voluntarily by an organization's decision.

1.2.2.1 Mandatory Audit

A mandatory or compulsory audit is an audit which is compulsory due to legislations. It basically is an obligation for certain types of organizations subject to audits. In mandatory audits, duration, purpose, terms on which audit would be carried out are determined by regulations and official statements. (Toroslu, 2012, p.70)

1.2.2.2 Voluntary Audit

Voluntary audits are audits which are performed to evaluate the current status of organizations. They are not legally required, but companies voluntarily prefer them to be conducted. (Akgül, 2000, p.13)

Limits of such audits are determined by those who demand it. Similar to mandatory audits, the auditor is obliged to follow necessary professional attention and care in voluntary audits. Therefore, there is no difference between mandatory audits and voluntary audits in terms of practice. (Akgül, 2000, p.68)

1.2.3 Audits Classified on the Basis of Auditor Status

1.2.3.1 Independent/External Audit

BRSA defines independent audit as a process which examines the reliability and accuracy of accounts, recording procedures and financial statements at banks. It also investigates the relevance of financial statements, recording procedures and financial statements to banking regulations. Furthermore; independent audit requires the auditor to collect audit evidence to be delivered to the related parties. Finally, the process requires the auditor to evaluate evidence collected and report all of the results. (Banking Regulation and Supervision Agency (BRSA), 2006, p.3) http://www.bddk.org.tr/WebSitesi/turkce/Mevzuat/Bankacilik_Kanununa_Iliskin_Duzenlemeler/140131677bagimsiz_denetim_islenmis_nihai_webe_basbakanliktan_sonra.pdf

CMB (Capital Markets Board) reviews financial statements which will be presented to the public. CMB defines independent audit as the examination of financial statements for ensuring their compliance with generally accepted accounting principles, concepts and standards. It also requires verification of information by checking records and documents and also reporting the findings. (Ceylan and Korkmaz, 2008, p.494)

1.2.3.2 Internal Audit

An organization's risk management and governance can be evaluated effectively via an internal audit. Internal audit can also be used to determine the efficiency of an organization's internal control processes. Internal audit provides independent assurance in all of these matters.

Internal audit is mainly concerned with evaluating an organization's management of risk. There are various examples of risk which today's organizations face in the world. For example, an organization's reputation might get damaged if it treats its customers unfairly. There are always health and safety risks in organizations. Organizations who depend on suppliers also might experience different kinds of risks. Furthermore; there are risks associated with market failure and cyber security in some organizations. Finally, all of the organizations in the world continuously experience financial risks. The key to an organization's success is being able to manage these different kinds of risks effectively. Organizations dealing with risks more effectively than their competitors would be more successful. (Institute of Internal Auditors (IIA), 2015) https://www.iia.org.uk/about-us/what-is-internal-audit/#what

The differences and similarities between external and internal audit are summarized in the table below:

Table-1: The Differences and Similarities Between Internal and External Audit (Institute of Internal Auditors (IIA))

	External Audit	Internal Audit
Reports To	Shareholders or members who are outside the organizations' governance structure.	The board and senior management who are within the organizations' governance structure.
Objectives	Add credibility and reliability to financial reports from the organization to its stakeholders by giving opinion on the report.	Evaluate and improve the effectiveness of governance, risk management and control processes. This provides members of the boards and senior management with assurance that helps them fulfill their duties to the organization and its stakeholders.
Coverage	Financial reports, financial reporting risks.	All categories of risk, their management, including reporting on them.
Responsibility for Improvement	None, however there is a duty to report problems.	Improvement is fundamental to the purpose of internal auditing. But it is done by advising, coaching and facilitating in order to not undermine the responsibility of management.

1.2.3.3 Governmental Audit

Governmental audit is a type of audit performed by certain governmental auditing units. These institutions are assigned and authorized by law and perform their audits in line with such laws. Auditing institutions performing auditing duties are; State Supervisory Council and Turkish Court of Accounts. There are also auditing boards connected to government institutions. (Kepekçi, 2000, p.4)

1.3 AUDITOR TYPES

An auditor is an unprejudiced and reliable individual who has professional knowledge and experience in auditing and who is able to perform any operation related to auditing.

1.3.1 Independent Auditors

Independent auditors are generally employed by auditing companies to provide professional auditing services to organizations. Independent auditors perform financial statement audits, compliance audits and operational audits. (Güredin, 2000, p.9)

1.3.2 Internal Auditor

Internal auditor helps executive management and boards to ensure that they are managing the company efficiently on behalf of their shareholders. The main purposes of internal audit are to improve and protect organizational value by providing risk-based and objective assurance, recommendation and insight.

Internal auditors deal with issues fundamentally important to the organizations so that they can survive and succeed. Unlike external auditors, internal auditors look beyond financial risks and statements. They consider wider issues like the organization's reputation, growth, impact on environment and how it treats its employees. (Institute of Internal Auditors (IIA), 2015)

Internal auditors have to be independent and unbiased. Their employers value them since they provide an independent and objective view. For this purpose, they need exceptionally wide range of skills and knowledge. (Institute of Internal Auditors (IIA), 2015) https://www.iia.org.uk/about-us/what-is-internal-audit/#what

1.3.3 Governmental Auditors

Governmental auditors work for government organizations and perform audits on behalf of them. Governmental auditors audit not only the operations of private organizations but also government organizations. These audits are performed based on laws, regulations and general policies. (Ulusoy, 2007, p.102)

CHAPTER 2

INTERNAL AUDITING

2.1 DEFINITION OF INTERNAL AUDIT

The Institute of Internal Auditors (IIA) is an organization for professional internal auditors. IIA defines practice of internal auditing as independent assurance and consulting activity conducted within organizations to examine and evaluate their activities as a service to their organization.

The remainder of the IIA's definition for internal auditing includes a number of important terms which applies to the profession:

• Independent means free from restrictions which could significantly limit the scope and effectiveness of the review or later reporting of resultant findings and conclusions.

• Appraisal confirms the need for an evaluation which is the main motivation for internal auditors as they develop their conclusions.

• Established supports that internal audit is a formal, definitive function in current organizations.

• Examine and define active roles of internal auditors, for fact-finding inquiries and for judgmental evaluations.

• Its activities verify broad jurisdictional scope of internal audit work which applies to all activities at modern organizations.

• Service reveals that help and assistance to management and other members of the organization are the end products of all internal auditing work.

• Verifies to the organization that internal audit's total service scope applies to the entire organization, including personnel, board of directors and audit committee, shareholders and other relevant stakeholders. (Moeller, 2005, pp.3-4)

ECIIA stands for The European Confederation of Institutes of Internal Auditing. ECIIA defines;

"Internal auditing as an independent, assurance and consulting activity designed to add value and enhance an organization's operations. It helps an organization achieve its objectives by bringing a systematic, disciplined approach to evaluate and increase effectiveness of risk management, control and governance processes." (The European Confederation of Institutes of Internal Auditing (ECIIA), March/2016) http://www.eciia.eu/what-we-do/what-is-internal-auditing/

2.2 HISTORY OF INTERNAL AUDITING

Known as the "founder" of modern internal auditing, Lawrence B. Sawyer, stated that internal auditing developed as an accounting-based profession and evolved systematically due to macroeconomic trends and developments in international trade. Sawyer also mentioned that modern internal auditing history is changed by the transfer of the recording and auditing system from Great Britain to USA, developed during the industrial revolution. (Özbek, 2012, p.6)

During the audits performed in accordance with "Securities Act" of 1933 and "Securities Exchange Act" of 1934 for securities offered to public in USA, accounting and auditing requirements by companies for the accuracy and reliability of accounting records have revealed that independent auditing would not be sufficient alone. Therefore, enterprises began to create internal auditing units. Although the

profession of external auditing has a long history, internal auditing came to prominence after 1940s. (Gürbüz, 1995, p.50)

In USA, Foreign Corrupt Practices Act of 1977 (FCPA) proposed that transactions of publicly-traded companies should be performed by authorized people and there should be internal control mechanisms to provide sufficient assurance for financial activities and accounting recording systems.

Due to the fact that establishing an internal audit department is one of the easiest ways to meet the requirements of the above-mentioned law, many companies developed their own internal auditing departments or increased the quality of their existing internal auditing departments.

Although there are no other legal regulations, companies voluntarily developed their own internal auditing departments due to its benefits. (Akarkarasu, 2000, p.16)

Among international internal auditing institutes, there are 3 prominent institutions which help create and strengthen internal auditing system in the world.

2.2.1 The Institute of Internal Auditors (IIA)

The foundation of "The Institute of Internal Auditors" (IIA) in 1941 in USA was a milestone for the improvement of modern internal auditing activities. IIA has continued to be a pioneer for the internal auditing profession to reach its current status through studies for defining the basic principles, standards, and ethics.

After the foundation of IIA, particularly during post World War II; goals of internal auditing practices rapidly changed. It became no longer an extension of independent auditing, its scope exceeded and extended beyond the boundaries of financial reports

and accounting system, and also included auditing of the effectiveness and efficiency of internal control systems and company operations. (Özbek, 2012, p.17)

2.2.2 European Confederation of Institutes of Internal Auditing (ECIIA)

Established in 1982, ECIIA is a professional body having members of internal auditing institutes operating in 33 European countries. The purpose of this confederation is to introduce internal auditing profession, its benefits, standards and characteristics in member countries, and ensure that International Internal Auditing Standards and ethics are applied in private and public areas.

For this purpose, it conducts researches, publishes reports, delivers conferences and provides consultancy on issues related to the profession. It is the permanent consultant for European Commission on services related to internal auditing. (The European Confederation of Institutes of Internal Auditing (ECIIA), March/2016) http://icdenetim.kultur.gov.tr/TR,46902/mesleki-kuruluslar.html

2.2.3 Chartered Institute of Internal Auditors (England and Ireland)

Established in 1948, Chartered Institute of Internal Auditors (England and Ireland) is an institute known in the fields of risk management, corporate management and internal control. The Institute aims to keep the interests of internal auditing at the top level, to increase the number of internal auditors in the world and to respond to training needs in the related areas. (Abdioğlu, 2008, p.91)

We can distinguish Turkish professional institutions as follows:

- The Institute of Internal Auditing - Turkey was founded in September 19, 1995 for development of internal audit profession in Turkey in conformance with international standards. The Institute of Internal Auditing offers different services for the development of professional skills and competence. It also intends to increase corporate governance quality of both financial and non-financial companies and relevant public entities as well as academic development of the profession. (The Institute of Internal Auditing - Turkey (TIDE), March/2016) https://www.tide.org.tr/uploads/brosurrbaski.pdf

- Public Internal Auditors Association (KIDDER) was established to meet the requirements of its members in professional, economic, social and cultural fields, to protect and support their rights and interests, to help resolve their professional problems, to create a common platform for performing public sector internal auditing activities in a competent, honest and independent manner and for improving the profession of internal auditing, to support its members on these issues, and to perform or have others perform professional and scientific studies. (Public Internal Auditors Association (KIDDER), March/2016) http://icdenetim.kultur.gov.tr/TR,46902/mesleki-kuruluslar.html

2.3 INTERNAL AUDITING STANDARDS

Internal auditing standards published by IIA points to a process of approximately 65 years of change and improvement. Internal auditing was mainly perceived as an extension of independent external auditing for financial reports in the years IIA was established. However Brink, one of the founders of IIA, mentioned concept of “operational audit” in 1958 for the first time and said “We, as employees of the company, give critical importance to all company operations and are deeply

interested in helping to have such operations as profitable as possible". This change increased the studies for defining the responsibilities of internal auditing. (Özbek, 2012, p.49)

Standards provide guidance on how to fulfill internal auditing requirements both for the institution and the auditor. Standards define the nature of internal auditing operations, key items of internal auditing regulations and annual activity plans, principles of duty performance, evaluations and criteria for quality used to assess performance of services. (Aslan, 2010, p.82)

Breakdowns of Attribute Standards and Performance Standard are given below. (The Institute of Internal Auditors (THEIIA), March/2016, pp.3-18) https://na.theiia.org/standards-guidance/Public%20Documents/IPPF%202013%20English.pdf

2.3.1 Attribute Standards

1000 – Purpose, Authority, and Responsibility

1010 – Recognition of the Definition of Internal Auditing, the Code of Ethics, and the Standards in the Internal Audit Charter

1100 – Independence and Objectivity

1110 – Organizational Independence

1111 – Direct Interaction with the Board

1120 – Individual Objectivity

1130 – Impairment to Independence or Objectivity

1200 – Proficiency and Due Professional Care

1210 – Proficiency

1220 – Due Professional Care

1230 – Continuing Professional Development

1300 – Quality Assurance and Improvement Program

1310 – Requirements of the Quality Assurance and Improvement Program

1311 – Internal Assessments

1312 - External Assessments

1320 – Reporting on the Quality Assurance and Improvement Program

1321 – Use of "Conforms with the International Standards for the Professional Practice of Internal Auditing"

1322 – Disclosure of Nonconformance

2.3.2 Performance Standards

2000 – Managing the Internal Audit Activity

2010 – Planning

2020 – Communication and Approval

2030 – Resource Management

2040 – Policies and Procedures

2050 – Coordination

2060 – Reporting to Senior Management and the Board

2070 – External Service Provider and Organizational Responsibility for Internal Auditing

2100 – Nature of Work

2110 – Governance

2120 – Risk Management

2130 – Control

2200 – Engagement Planning

2201 – Planning Considerations

2210 – Engagement Objectives

2220 – Engagement Scope

2230 – Engagement Resource Allocation

2240 – Engagement Work Program

2300 – Performing the Engagement

2310 – Identifying Information

2320 – Analysis and Evaluation

2330 – Documenting Information

2340 – Engagement Supervision

2400 – Communicating Results

2410 – Criteria for Communicating

2420 – Quality of Communications

2421 – Errors and Omissions

2430 – Use of "Conducted in Conformance with the International Standards for the Professional Practice of Internal Auditing"

2431 – Engagement Disclosure of Nonconformance

2440 – Disseminating Results

2450 – Overall Opinions

2500 – Monitoring Progress

2600 – Communicating the Acceptance of Risks

2.4 REASONS FOR PERFORMING INTERNAL AUDITS

Reasons for performing internal audits in an organization can be summarized as follows: (Aslan et al., 2006, pp.8-13)

- Responsibility and Accountability

In enterprises, managers assign part of their responsibilities and powers to their employees so that work gets completed faster and becomes more effective. Internal auditors basically evaluate how managers in all levels perform their duties, including senior managers, on behalf of board of directors. This way, internal auditors meet the needs of board of directors to support them with objective and reliable information.

- Agency Theory

As the scale of companies grow, the need for management by professionals increase. The connection between company owners and company managers are deemed as agency contracts. It is important for company owners, that managers, who are acting on behalf of company owners, use resources effectively and efficiently. Internal auditing plays an important role in this matter.

- Consultancy and Assistance to Management

Internal auditors, as well as detecting errors and frauds at organizations, also help management to determine the potential error and fraudulent transactions there could have taken place and what can be done to prevent them.

- Necessity for Protection against Fraudulent Transactions

Development of financial instruments and financial markets, company transactions became more complex. As a result, it became harder to detect existing or prospective irregularities. Internal audit is important to prevent damage due to these applications.

2.5 PURPOSE AND SCOPE OF INTERNAL AUDITS

Although having an internal auditing function is a necessity for companies quoted in stock exchanges, banks and other financial institutions and many small, medium and large-scale enterprises have internal auditing functions. Internal auditing is perceived as a valuable part of the administrative control that provides assurance to audit committee and management, and is regarded as a function which adds value to the credibility of the enterprise for investors and creditors. (Fraser and Lindsay, 2005, p.21)

The definition of internal auditing states the fundamental purpose, nature, and scope of internal auditing. “Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.” (The Institute of Internal Auditors (THEIIA), April 2016, para.1-2) https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Definition-of-Internal-Auditing.aspx

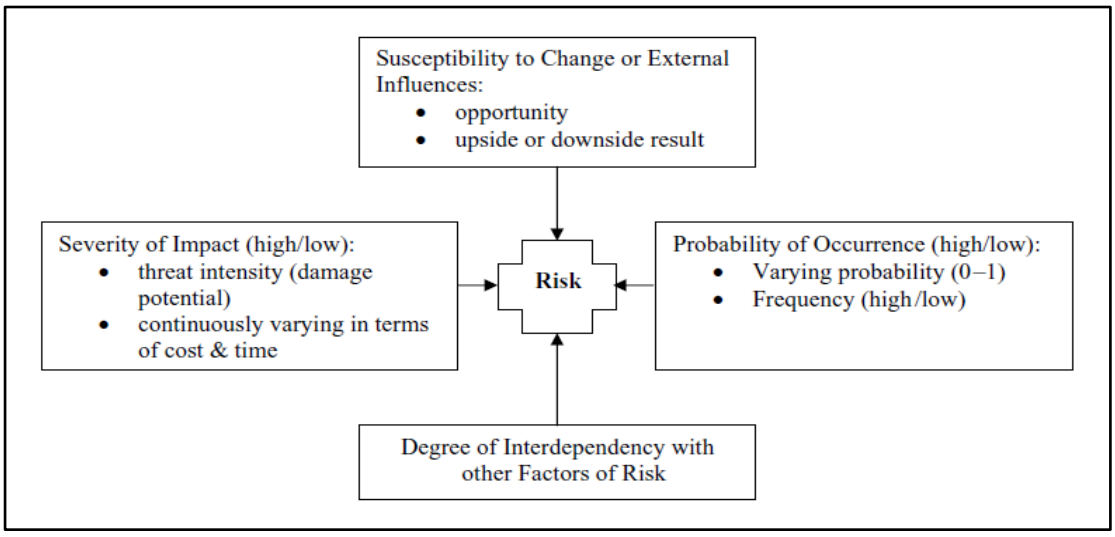
CHAPTER 3

ENTERPRISE RISK MANAGEMENT ASSESSMENT

3.1 DEFINITION OF RISK

The term ‘risk’ is used to imply a calculation of probability of an outcome, the size of the outcome or a combination of both. There have been some efforts to include the idea of both size and probability of an outcome in one single definition. (Merna and Al-Thani, 2005, pp.9-10)

Figure-1: Typical Risk Parameters (Merna and Al-Thani, 2005, pp.9-10)



From another point of view, risk can also be defined as the threat resulting from an action or event which will adversely affect an organization’s ability to accomplish its objectives and execute its strategies successfully.

This definition highlights some key elements:

1. Risk is perpetually a threat; something that might happen.

2. Threat relates to an event that has to occur for the risk to materialize.

3. Event, if happens, will affect the success of business objectives. (Griffiths, 2005, p.17)

As much as risk contains threat of damage, it also contains opportunities, thus it is narrow to see risk from only a negative point of view. (Keskin, 2006, p.16) Risk can only be minimized, but it cannot be fully eliminated. (Pehlivanlı, 2010, p.59)

3.2 CLASSIFICATION OF RISKS

Developments and changes in developing industries require risks to be monitored and managed more carefully. It is not possible to create a risk classification that can be applied to all enterprises. That's way, auditors should work together with company management to develop a classification for various risks for that company and to measure the risks of the company. (Roth and Espersen, 2002, p.18)

Generally, risk types can be classified as follows. (Kır, 2010, pp.53-54)

3.2.1 Inherent Risk

It is a type of risk that might happen when management does not take any precautions and does not take any action against adversities. In other words, it is the possibility of having serious problems and irregularities in a work or transaction when there are no internal control procedures.

3.2.2 Control Risk

It is a type of risk faced in case there are no appropriate internal controls or internal controls are not applied appropriately. In other words; it is the possibility that critical errors and irregularities in a transaction might not be revealed by internal control system.

3.2.3 Residual Risk

It is a type of risk that remains after the precautions (control activities) taken by management to eliminate possibility of adversities to happen and to mitigate impact of adversities in case they can not be eliminated. This is also known as "vulnerability" and it is residual risk that remains after inherent risk.

Risks can be classified as; credit risk, operational risk, market risk, reputational risk, interest rate risk, foreign currency rate risk, liquidity risk and country risk. (Kır, 2010, pp.53-54)

3.3 DEFINITION OF RISK MATRIX

Risk matrix is a dynamic analysis tool used for presenting an organization's risk status based on its activities, effectiveness of risk management systems, net risk level and the changes in the risk levels. Low levels of risk (acceptable) and high levels of risk (unacceptable) are treated differently, as the aim is to determine which risks should have a priority as a result of the risk assessment. Top priority risks are more urgent and are subject to detailed examination. (Benli and Celayir, 2014, p.14)

Probability and impact matrix uses the combination of probability of risk occurrence (likelihood) and impact scores of risks. Generally, a 3x3 matrix or a 5x5 matrix is used and a sample matrix of 5x5 is presented below: (Probability and Impact Matrix, 2012, para.2-4, http://www.justgetpmp.com/2012/02/probability-and-impact-matrix.html)

		Impact				
		Trivial	**Minor**	**Moderate**	**Major**	**Extreme**
Probability	**Very Unlikely (Rare)**	Low	Low	Low	Medium	Medium
	Unlikely	Low	Low	Medium	Medium	Medium
	Moderate	Low	Medium	Medium	Medium	High
	Likely	Medium	Medium	Medium	High	High
	Very Likely	Medium	Medium	High	High	High

3.4 RISK MANAGEMENT

Risk management can be defined as any set of actions taken by individuals or business organizations in an effort to reduce risk arising from their business. Risk management deals both with insurable and uninsurable risks. It is an approach that involves a methodical process for systematically identifying, analyzing and responding to risk events throughout the life of a project. (Merna and Al-Thani, 2005, p.35)

Risk management can be considered a 4 step process: (Moeller, 2007, p.22)

1. Risk identification

2. Quantitative or qualitative estimation of documented risks

3. Risk prioritization and response planning

4. Risk monitoring

Predicting an incident before it happens and determining what to do against it is the best way for minimizing the potential adversities and maximizing the opportunities. This is directly related to the success of an institution and it is the subject of risk management. The advantages of risk management can be summarized as follows: (Derici et al., 2007, pp.153-154)

- Minimizes surprises and losses,

- Helps taking fast and effective decisions,

- Saves time,

- Prevents wasting resources,

- Helps keeping risks at reasonable levels,

- Encourages people for being open to innovations.

Risk management and internal control are strongly related to the capability of businesses to accomplish clear corporate objectives. Accepting risk management in this way will help to assure our focus on opportunities and also it will help us deal with possible threats. Hence, it is essential to integrate risk management in the planning process. (Griffiths, 2005, p.21)

3.5 ENTERPRISE RISK MANAGEMENT

Enterprise Risk management (ERM) is a process which is affected by an entity's board of directors, management and other personnel. ERM is applied within a plan across an enterprise. It is designed to identify possible events which may affect the

entity and manage risk to be within its risk appetite. It also needs to provide reasonable assurance regarding achievement of entity objectives.

Key points to acknowledge when using COSO ERM involve: (Moeller, 2007, pp.50-52)

• Enterprise Risk management is a process, where process is defined as a set of action designed to achieve a result.

• ERM process is implemented by people in organizations.

• ERM is administered through the setting of strategies across all organization.

• The concept of risk demand must be acknowledged.

• ERM is designed to accomplish success of objectives.

With Sarbanes-Oxley Law, enacted in 2002 in USA, imposing obligation to make structural reforms for many companies, lawmakers developed practices against corporate scandals, which became common in public opinion. Furthermore, effective "Enterprise Risk Management (ERM)", more consistent, extensive and economical management of potential risks, has become more critical. (PWC, 2006, p.4)

Briefly, one advantage of ERM is that it enables a consistent and optimal risk management for institutions, where related risks found in different units with various effects. Another advantage of ERM is creation of common risk perception throughout the institution. (PWC, 2009, p.11)

3.6 COSO "ENTERPRISE RISK MANAGEMENT–INTEGRATED FRAMEWORK"

COSO produced an excellent set of guidance notes named “Enterprise Risk Management – Integrated Framework” in 2004. These guidance notes provide a benchmark for organizations to help assess the efficiency of their approach to risk management in the organization. “Application Techniques” and “Enterprise Risk Management - Integrated Framework” documents provide a very broad explanation of Enterprise Risk Management. (Griffiths, 2005, p.41)

An extensive approach to risk management throughout the entire institution, although not a requirement to manage individual risks, allows the institution to acquire maximum benefits from risk management activities, allows the performance of risk management operations, and also, allows monitoring and evaluation of its effectiveness. The point reached in risk management is integrated risk management system, where all risks are gathered under a single roof. (Bolgün and Akçay, 2003, p.414)

Committee of Sponsoring Organizations of the Treadway Commission (COSO) released the original Internal Control - Integrated Framework in 1992. The original framework has gained extensive acceptance and it was universally used around the world. This framework is perceived as a leading framework to design, implement and administer internal control. It is also used to assess effectiveness of internal control. (COSO, 2013, p.1)

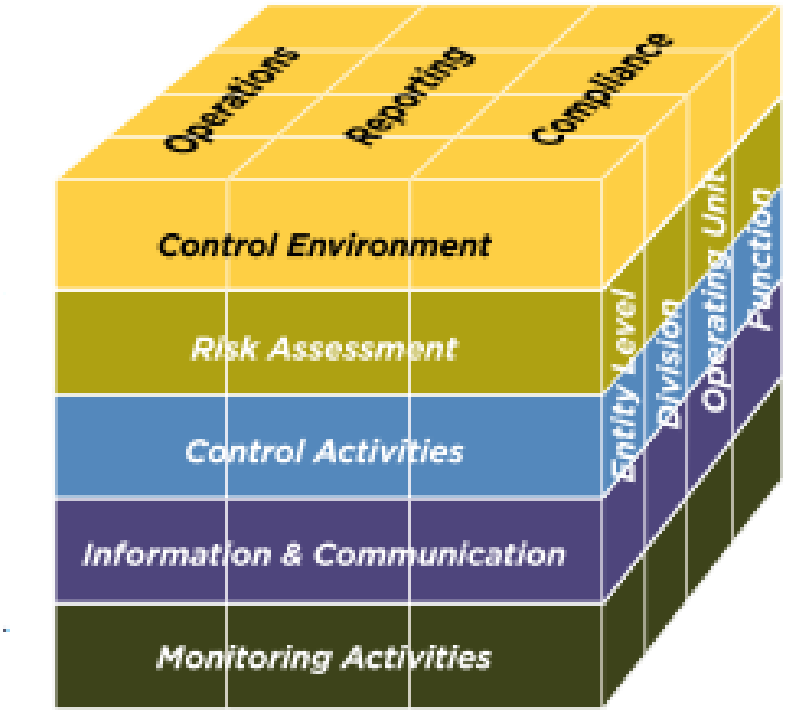
Internal Control - Integrated Framework published by COSO helped many institutions in both private and public sectors to establish and improve internal control systems. However, due to increase in operational volumes in recent years, the concept of risk has become gradually more prominent, and a strong framework has become necessary to effectively evaluate and manage risks.

For this purpose, in 2001, COSO and Pricewaterhouse Coopers prepared a study for risk managers. With the operational scandals revealed in the same period; investors, shareholders and employees incurred losses. These scandals increased the need for

new laws, regulations and standards in corporate management and risk management. For this purpose, COSO published “Enterprise Risk Management - Integrated Framework” in 2004. (Saltık, 2007, p.21)

The COSO framework is illustrated in the form of a three-dimensional cube with following elements:

Figure-2: COSO Cube



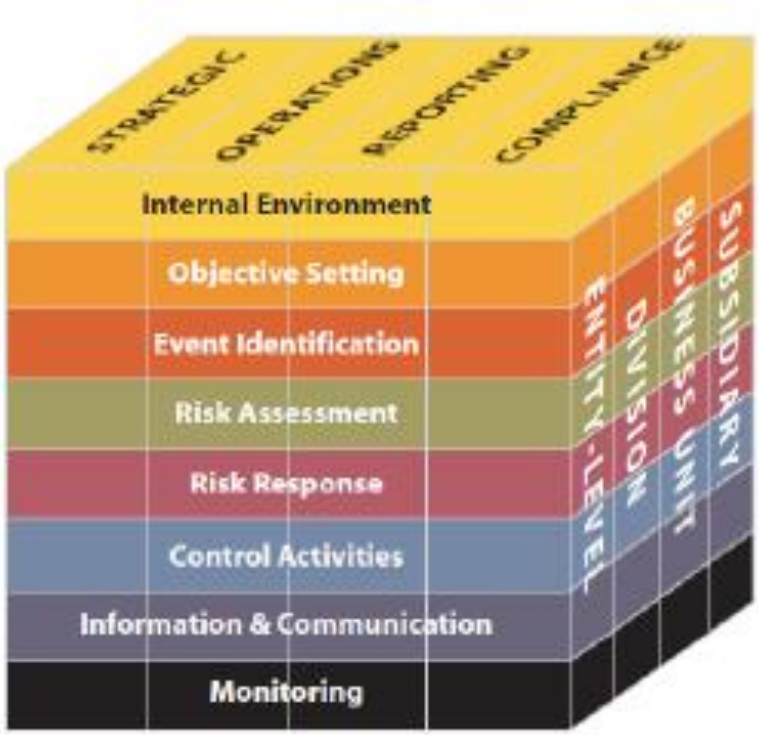
In COSO Cube, a direct relationship exists between objectives and components. Objectives are what an entity strives to achieve. Components represent what is required to achieve the objectives and the organizational structure of the entity. The relationship between objectives and components can be shown in a form of cube.

• 3 categories of objectives namely operations, reporting and compliance are represented as columns

• 5 components are shown as rows

• An entity's organizational structure is represented by third dimension. (COSO, 2013, p.2)

Figure-3: COSO ERM Framework



The relationship between objectives and components are shown in a form of cube.

• 4 categories of objectives are strategic, operations, reporting and compliance which are represented in columns.

• 8 components are internal environment, objective setting, event identification, risk assessment, risk response, control activities, information & communication and monitoring activities which are presented in rows. These components represent what is needed to achieve the four categories of objectives.

• An entity's organizational units are represented by the third dimension which shows the ability of the model to focus on parts of the organization as well as the whole. (ACCA, COSO Enterprise Risk Management Framework, The ERM Model, May 2017 para.1-2) http://www.accaglobal.com/uk/en/student/exam-support-resources/professional-exams-study-resources/p1/technical-articles/coso-enterprise-risk-management-framework-part-1.html

First of all, an entity has to select a strategy and establish aligned objectives cascading through itself. These objectives are set in four different categories. Strategic objectives are high-level goals, which supports its mission. Operational objectives enable an efficient and effective use of entities' resources. Reporting objectives guarantee the reliability of the reporting system. Compliance objectives need to meet all legal and regulation requirements. (Kerstin et al., 2014, pp.3-4)

3.7 MAIN ISSUES RELATED TO ENTERPRISE RISK MANAGEMENT

According to COSO report, ERM description has the following features: (Saltık, 2007, pp.21-22)

- ERM is a continuously working process.

- It is affected by each employee at all levels of the institution.

- It is used to define business strategies.

- It aims to minimize operational surprises and losses through effective and active monitoring.

- It reduces the possibility of occurrence of adverse incidents, aims to protect and improve the reputation of the institution by utilizing opportunities as much as possible.

- It provides reasonable assurance for executive managers and board of directors.

- It defines possible incidents which can affect an enterprise and manages risks which are more likely to happen.

- It ensures that corporate efficiency is increased through more effective practices.

- It allows targets are achieved by various matching categories.

3.8 BENEFITS OF ENTERPRISE RISK MANAGEMENT

Benefits of ERM for enterprises can generally be summarized as follows: (Bozkurt, 2010, pp.22-23)

- Decision making and planning are based on more robust data.

- Increase in opportunities and possibilities for change.

- Preventing unpredictable situations and being ready for risks.

- Creating more strong, effective and target-driven strategies.

- Accessing fastly to more effective risk information.

- Detecting opportunities and threats better beforehand.

- Creating opportunities and values out of uncertainties.

- Increasing service presentation quality.

- Adapting proactive management style instead of reactive management.

- Using resources and allocations more effectively.

- Managing incidents better to reduce costs of losses and risks.

- Achieving continuity in compliance and conformity to legislations and other procedures.

- Monitoring performance based on risk.

- Contributing to improvement of corporate management.

- Creating more possibilities to reach goals.

3.9 RELATIONSHIP BETWEEN ENTERPRISE RISK MANAGEMENT AND INTERNAL AUDITING

Audit plans should be made by focusing on the greater areas of risk and risks should be assessed when programming internal audits and implementing internal auditing practices. For carrying out audit processes in a better and more effective way, existing or potential risks should be defined, evaluated and necessary controls should be improved. In this context, risk and risk management have become the most important issues for internal auditors. (Özaydın, 2010, p.32)

Internal auditing contributes to ERM processes in various ways, in both conventional and consultant roles. As known, boards of directors have the final responsibility on risk management. In line with authorizations by board of directors, risk detection and management are among the main responsibilities of senior management. (Kurtoğlu, 2004, p.22)

Internal auditing also affects efficiency in enterprise operations. In this context, it is observed that ERM and internal auditing present a common approach for reaching the same purpose.

The roles of internal auditing with regard to ERM are providing assurance on the issue of risk management processes, providing assurance on whether risks are accurately measured and evaluated, measuring and evaluating risk management processes, assessment of reports on important risks, and reviewing management of important risks.

The objectivity and independence of internal audit is an important issue. If there are ERM processes perceived to impair independence of internal auditors, internal auditors should not take part in such processes. It should be fully understood by the management of organizations that risk management responsibility rests with them.

Having an active role in development and management of a risk management process is not the same as the role of “undertaking the responsibility of risks”. Therefore, internal auditors should avoid the role of “undertaking the responsibility of risks”. (Bozkurt, 2010, pp.24-26)

CHAPTER 4

RISK-BASED INTERNAL AUDITING AND ITS ROLE IN THE BANKING SECTOR

4.1 RISK-BASED INTERNAL AUDITING

4.1.1 The Concept of Risk-Based Internal Auditing

Today, approaches of companies to risk is quite different than what it was in the past. While risks were avoided in the past, now, benefiting from risky activities is in the forefront. Following the global crisis experienced, limitless risks taken previously became questionable and useful improvements were implemented to manage such risks. These developments connected with risks make it necessary for entities to audit risks undertaken as a result of risk management. (Kishalı and Pehlivanlı, 2006, p.75)

Risk based audit is a process, a set of procedures and an attitude of mind rolled into one. The simplest way to define risk based audit is that it is an audit that matters most to an organization. (Griffiths, 2005 p.5)

Risk based internal auditing provides an unbiased and independent opinion to an organization's management as to whether the related risks are being managed sufficiently or not.

The methodology consists of the five core internal audit roles covering the risk management framework of all organizations:

1. Ensuring that processes implemented by management to identify all important risks are efficient.

2. Assuring that risks are correctly evaluated by the management in order to prioritize them.

3. Assessing risk management processes to assure that applicable risk responses comply with the policies of the organization.

4. Evaluation of the risk reports by management.

5. Reviewing the risk management process to assure that controls have been implemented and are being monitored. (Griffiths, 2006, pp.1-2)

In case of risk-based internal auditing, first, risk status is uncovered. Scope, content, timing of the internal auditing activity and allocation of resources are shaped according to risk status. The risk-based internal auditing plan is prepared by identifying and assessing risks that entities will be exposed to. As a result of the risk management processes conducted, high risk areas of the entity are determined and a customized audit system is designed according to these areas. (Aksoy, 2006, p.1479)

The risk-based internal auditing is a recent term which focuses on future activities rather than past activities. Risk-based auditing is a systematic approach incorporating all audit and review techniques, including traditional audit and review techniques which have the objective of identifying risk profiles of entities. (Adiloğlu, 2011, p.67)

4.1.2 Difference between Traditional Internal Auditing and Risk-Based Internal Auditing

Risk-based internal auditing approach and traditional internal audit approach are assessed in a comparative manner.

In a classical approach, benefit/cost analysis does not take priority; instead the focus point of auditing becomes detection of the issues and deficiencies in an audit and then eliminating them. (Tokkder, April/2016), http://tokkder.org/tokkder-dergi/1080

The risk-based internal auditing is based on assumptions whereby auditing resources are not infinite, activities of the unit to be audited are exposed to different risks and have relatively different degrees of importance. Under the light of these assumptions, the internal audit manager prepares plans based on prioritizing of the internal auditing activities in accordance with targets of the organization and puts such plans into action. (Kishalı and Pehlivanlı, 2006, p.79)

This process shows how it has developed assuming a higher profile and a greater degree of professionalism. This type of audit service has changed to demonstrate these new possibilities. These developments may similarly be traced: (Pickett, 2003, pp.10-11)

- Internal check measures

- Transaction based approach

- Statistical sampling

- Honesty based work

- Spot checks

- Risk analysis

- Systems based approach

- Operational audit

- Management audit

- Risk-based auditing

4.1.3 Scope and Objective of Risk-Based Internal Auditing

Risk-based internal auditing aims effectiveness, efficiency and specialization at auditing. It depends on whether internal audit and risk management systems are working adequately and reliably. It also depends on existing weaknesses in systems. This approach whereby form and scope of the auditing and allocation of auditing resources are identified based on risk status includes constant monitoring, assessment of risk profiles of entities and taking necessary measures. (Kurnaz and Çetinoğlu, 2010, p.138)

The main purpose of the risk-based internal auditing is to provide indepented assurance to the board of directors on the issues listed below:

- Whether risk management processes implemented by the management across the organization are carried out in the intended manner or not,

- Whether the aforementioned risk management processes have a sound and consistent design or not,

- Whether the measures taken by the management against potential risks are sufficient and efficient or not,

- Whether structured a sound and consistent control framework connected with measures taken by the management against potential risks is established or not. (Göğüş, 2012, p.47)

4.2 RISK-BASED AUDITING PROCESS

The risk-based auditing approach is a methodology that refers to the detection of risks of the operations of a company and allows to provide assurance to the board that such risks are managed effectively through appropriate techniques. The risk-based auditing process is composed of the following activities: (IIA, 2003, p.1)

- Identification of the Entity's Risk Maturity through Risk Assessment
- Preparation and Approval of the Auditing Plan
- Conducting the Audit
- Audit Conclusions and Reporting
- Assessing the Results of an Audit

4.2.1 Identification of the Entity's Risk Maturity through Risk Assessment

4.2.1.1 Risk Assessment

Risk assessment is the level where risk, which constitutes the main point of risk-based auditing, is identified. Attention should be paid for the following topics for the success of the risk assessment: (Eşkazan, 2005, p.33)

• Risk assessment model should be designed according to the requirements and needs of the organization and should be kept as simple as possible.

• When it comes to risk assessment, people may rely on their instincts as well as facts. Assessment should have a meaning for the auditor.

• The key to a successful risk assessment process is understanding and diagnosing risk by the internal auditor.

• Managers should take part in risk assessment.

• Risk assessment process should generate beneficial results acknowledged by both management and auditors.

Risk identification determines which risks can most probably affect the project and documents characteristics of each risk. Risk identification should include both internal and external risks. Main sources of risk that have potential to cause major effects on projects should be determined. They need to be classified according to their impact on time schedules, project costs and project objectives. (Merna and Al-Thani, 2005, p.38)

4.2.1.2 Prioritization

Prioritizing risks refers to classification of risks in terms of materialization range in terms of time and impact upon the entity's success. Levels of impact and probability are indicators of importance levels of risks. Risk with the highest priority is the one which is the most critical and has to be solved first. By deploying resources for the most critical risks, it is ensured that limited resources of the company are used effectively.

Also, it ensures that internal auditing resources are used most effectively and efficiently, helps determine priority order for areas to be audited and creates an effective auditing plan. (Pickett, 2003, pp.602-605)

4.2.2 Preparation and Approval of the Auditing Plan

Internal auditing activities are carried out by means of preparing plans annually. Preparing annual auditing plans in a risk-based manner is one of crucial regulations of standards. Here, the purpose is ensuring that limited resources of the internal auditing unit are used at the most risky areas of the entity. Annual auditing plans have to be prepared at least once a year, and they have to be reviewed as frequently as possible in proportion to risk level of the entity's operations. (Özbek, 2012, pp.807-808)

Well-designed audit plans have the following advantages: (Pickett, 2006, p.28)

- Improve stockholder confidence.
- Show a well use of audit budget.
- Increase corporate reputation.
- Reflect organizational values, goals and conduct.
- Boost auditors'motivation.
- Make sure that delivery of audit services has a major impact on organizations.
- Keep regulators pleased.
- Make life easier for external auditors.

4.2.2.1 Determination of the Auditing Population

The auditing population is affected by characteristics of the entity to an important extent, and, in general, may carry characteristics varying from entity to entity. The auditing population that may include components of the entity's strategic plan that generally reflects the targets of the entity. (Pehlivanlı, 2010, p.121)

The main purpose of internal auditing activities is to help materialize targets of the entity. Therefore, organizational structure, activity types and fields, basic targets for the current year of the entity will also have impacts upon targets of the internal audit. Apart from general targets stemming from the definition of the internal auditing activities and internal control concept, the entity's general targets connected with substantial company-wide changes planned by the company for that year will be taken into consideration while identifying general targets of the annual auditing plan. (Özbek, 2012, p.814)

Getting management's list of audit priorities is an essential step in developing an efficient audit plan. Most risks should be determined by the management. The risk register and the risk matrix will be invaluable in this situation. (Griffiths, 2005, pp.74-75)

4.2.2.2 Desired Level of Assurance

The level of assurance provided by internal audit is only additional rather than essential. The level of assurance can be improved by the use of computer assisted audit techniques.

In case there are any specific audits which require relatively higher level of assurance, management should be consulted like new activities such as e-commerce or areas

where concerns have been expressed. For these kinds of assignments, additional time will be needed to be factored into the plan. (Griffiths, 2005, p.76)

Scope of the audit and audit sampling will vary depending on the level of assurance. For instance, the level of assurance desired for areas with high degree of importance will be higher than that required for areas with a lower degree of importance. (Pehlivanlı, 2010, p.125)

4.2.2.3 Preparation of the Auditing Plan

The purpose of the risk-based auditing plan is to allocate auditing resources among those areas where effectiveness and probability combination of risk is the highest. The risk-based internal auditing plan;

- is a guide for the internal auditor,

- supports budget demands of the internal auditing,

- is a standard for measuring the internal auditors' own success,

- is an indicator that the internal audit activity is under expert control.

Risk assessment and risk-based internal auditing plan are important tools for achieving effectiveness and efficiency at the management of the internal auditing department. (Eşkazan, 2005, p.33)

The annual audit plan can be broken down into four quarters. Each defined audit can be tentatively assigned to a quarter. These quarters are April–June, July–September, October–December and January–March. The thirteen-week, quarterly planning period

is remarkably important in the current business environment. Quarterly planning is more meaningful than annual planning since organizations change very quickly and three monthly reviews can capture emerging risks much better than annual reviews. (Pickett, 2004, pp.159-160)

The internal auditor should develop an internal auditing plan based on levels of risks diagnosed in the process of risk assessment. The internal auditor should focus on high risk areas of the first degree which should be followed by risk areas of mid-degree and low-degree. (Kurnaz and Çetinoğlu, 2010, p.103)

4.2.3. Conducting the Risk-Based Internal Audit

4.2.3.1 Allocation of Engagement Resources and Engagement Work Program

According to IIA's internal audit performance standard 2230; internal auditors must allocate appropriate and sufficient resources to accomplish engagement objectives based on an evaluation of the nature and complexity of each engagement, available resources and time constraints. (The Institute of Internal Auditors (THEIIA), April/2016, p.14), https://na.theiia.org/standards-guidance/Public%20Documents/IPPF%202013%20English.pdf

The following issues should be explained in work programs to be generated as a result of duty program: (Pickett, 2006, pp.174-176)

• Identification: The engagement plan should identify which system or which aspects of a system are being reviewed. This decision will determine the beginning and end place of the system being "captured" by the auditor.

• Evaluation: The engagement plan should include information on how the system will be evaluated using appropriate techniques.

• Testing: The engagement plan might give some direction on the testing stage of the audit, including the use of computerized questionings using live or downloaded data.

• Documenting Information: The engagement plan should point out how audit findings will be communicated. The plan should state who will receive draft and final reports as a result of the engagement.

4.2.3.2 Identification and Implementation of Tests

Testing means gathering reliable evidence and comparing conformity of the incident, transaction or record audited with evidences in order to investigate whether or not the incident or transaction or the record audited is accurate and reliable. (Kepekçi, 2000, p.123)

An audit program is a procedure which describes procedures, steps and tests to be performed by the auditor during the audit. The program should be completed after the finalization of the preliminary and field surveys. It should be completed before starting the actual audit fieldwork. It should be formulated with several criteria. The most important criteria is that the program should describe the aspects of the area to be further examined and the sensitive areas which require audit emphasis. (Moeller, 2005, p.318)

4.2.3.3 Assessment of Test Results and Audit Findings

The most important finding of an audit is to understand that there is a nonconformity between the existing situation and the situation that is supposed to be happened. Such nonconformity may be affiliated with an erroneous transaction, a control practice that does not work as planned, a report that was not conveyed, a measure that has not been taken although it was required to be taken and legislation that has not been abided by although it was required by legislation. (Özbek, 2012, p.964)

Tests reveal whether controls are performed in connection with risks and implemented fully and sufficiently or not. Therefore, tests give an idea about accuracy of controls and effectiveness of the internal auditing. Results of conducted tests are indicated on auditing test matrix. (Pehlivanlı, 2010, p.133)

4.2.4 Audit Conclusions and Reporting

4.2.4.1 Preparation of Risk-Based Internal Auditing Report

Internal audit reports have various critical functions that should always be considered when completing audit work and delivering the results. Internal audit reports are generally formal written documents circulated to senior and higher management. They can also be informal or presented verbally at the end of the audit fieldwork. Either way, internal audit reports should always have four essential steps:

1. Disclosure of Findings.
2. Description of Findings.
3. Suggestions and Recommendations.
4. Auditor's Views and Comments. (Moeller, 2005, pp.404-405)

In case of risk-based internal auditing, goals of preparing internal audit report are as follows: (Griffiths, 2005, p.117)

- To deliver the conclusions of the audit in a professional manner.

- To give a proper level of assurance comparable with those observations.

- To make recommendations for improving risk management processes and controls.

- To determine overmanaged areas and unnecessary controls.

- To advise on possible balance between risk and control.

First of all, a well-prepared report should be submitted to related parties timely. A report not submitted on time loses its effectiveness and the solutions problems are delayed. The report should also be prepared with a focus on critical areas, in an accurate, concise and fluent manner, easy for readers to follow, clearly expressing the results and containing practical advices. (Pehlivanlı, 2010, p.137)

4.2.4.2 Preparation of the Draft Report

The draft report is a report containing general assessment and audit findings prepared by the internal auditor based on findings and evidences gathered from auditing tests applied during the auditing process in connection with effectiveness of internal control system and the unit audited with a view to achieving audit objectives. The main difference between the draft report and the final report is that the draft report prepared is sent to the managers of the unit audited for their comments and recommendations. (Özbek, 2012, p.999)

Final communication of engagement results should contain internal auditors' opinion and/or results according to IIA's internal audit standard 2410. When issued, a conclusion or an opinion must take account of the expectations of senior management,

the board and other shareholders. It should also be supported by sufficient, accurate, relevant and useful information. (The Institute of Internal Auditors (THEIIA), April/2016, pp.15-16), https://na.theiia.org/standards-guidance/Public%20Documents/IPPF%202013%20English.pdf

4.2.4.3 Preparation of the Final Report

The abovementioned draft report will be followed by a final report by the internal auditor once final comments of managers of the unit audited are added. The internal audit manager or an auditor appointed by her or him should review, approve the final audit report and should decide to whom the report should be distributed. If the report is sent electronically, a signed version of the report should be kept at the archive. (The Institute of Internal Auditing - Turkey, 2004, p.308)

4.2.5 Assessing the Results of an Audit

Internal audit activity does not get completed after individual auditing of the respective audit subject and sending the report to related parties. For completeness, results of internal audit activity should be followed. (Özbek, 2012, p.1013)

At every audit period, it should be controlled whether the findings of the previous period have been corrected through internal auditing programs or not. Those points uncorrected should be inquired and should be submitted to senior management within the internal audit report or in the form of a separate action plan as follow-up to the

final report. On the contrary, the senior management may take over risk of not correcting the problem or problems presented in the report due to costs or other reasons. (Göğüş, 2012, p.68)

4.3 CORE PRINCIPLES FOR EFFECTIVE BANKING SUPERVISION (THE BASEL CORE PRINCIPLES)

The Core Principles for Effective Banking Supervision (Core Principles) are the *de facto* minimum standards for solid practical supervision and regulation of banks and banking systems. It is originally issued by the Basel Committee on Banking Supervision (the Committee) in 1997. These principles are used by countries as a reference point for evaluating the quality of their administrative systems and for identifying future work to achieve a baseline level of solid administrative practices. These Core Principles are also used by the World Bank and the International Monetary Fund (IMF), in the context of the Financial Sector Assessment Programme (FSAP), to evaluate the efficiency of banking organizational systems and practices of countries.

Preventing bank failures should not be an objective of banking supervision. Nevertheless, supervision should aim to diminish the probability and impact of a bank failure. For this purpose, supervision should work with resolution authorities, in case failure occurs, it is in an orderly manner. (Bank for International Settlements (BIS), 2012, pp.1-13)

The 29 Core Principles are:

Supervisory powers, responsibilities and functions

Principle 1 – Responsibilities, objectives and powers

Principle 2 – Independence, accountability, resourcing and legal protection for supervisors

Principle 3 – Cooperation and collaboration

Principle 4 – Permissible activities

Principle 5 – Licensing criteria

Principle 6 – Transfer of significant ownership

Principle 7 – Major acquisitions

Principle 8 – Supervisory approach

Principle 9 – Supervisory techniques and tools

Principle 10 – Supervisory reporting

Principle 11 – Corrective and sanctioning powers of supervisors

Principle 12 – Consolidated supervision

Principle 13 – Home-host relationships

Prudential regulations and requirements

Principle 14 – Corporate governance

Principle 15 – Risk management process

Principle 16 – Capital adequacy

Principle 17 – Credit risk

Principle 18 – Problem assets, provisions and reserves

Principle 19 – Concentration risk and large exposure limits

Principle 20 – Transactions with related parties

Principle 21 – Country and transfer risks

Principle 22 – Market risks

Principle 23 – Interest rate risk in the banking book

Principle 24 – Liquidity risk

Principle 25 – Operational risk

Principle 26 – Internal control and audit

Principle 27 – Financial reporting and external audit

Principle 28 – Disclosure and transparency

Principle 29 – Abuse of financial services

4.4 STRUCTURE OF THE RISK-BASED INTERNAL AUDITING SYSTEM AT THE BANKING SECTOR

Banks are required to establish and operate sufficient and effective internal control, risk management and internal audit systems in harmony with their scope and structure of their activities. This also should respond to changing conditions and cover all their branches and undertakings. This needs to be done in order to monitor and control risks.

Board shall set the standards and procedures pertinent to the founding, functioning and adequacy of internal control, risk management and internal audit systems; the

activities to be accomplished; the units to be established; the responsibilities and obligations of senior management and the reporting to be made to the agency.

Internal control system

Within the scope of internal control system, banks shall (i) guarantee execution of activities in compliance with internal regulations, legislation and banking ethics; (ii) secure reliability and integrity of reporting and accounting systems and proper accessibility of information through regular control activities to be complied with and executed by the personnel at any level; (iii) guarantee the functional distribution of duties and sharing of powers and responsibilities the fund payments, the agreement of bank's transactions, protection of assets and control of liabilities; (iv) identify and assess any risk encountered and prepare the infrastructure required for managing such risks; and (v) establish a convenient information exchange network. Internal control activities shall be executed by the internal control personnel and the internal control department reports to the board of directors. (Banking Law no.5411, 2013, pp.44-45), https://www.bddk.org.tr/websitesi/english/Legislation/14905banking_law_december_2013.pdf

Risk management system

Banks shall establish, implement and report risk policies within the framework of the principles set by the Board and within the scope of risk management system. Risk management activities shall be performed by the risk management department and personnel to work under the board of directors.

Internal audit system

Banks shall establish internal audit systems which include all their branches, units and subsidiaries subject to consolidation. In this context, bank auditors shall investigate the compliance of the banking activities to the legislations, articles of association, internal regulations and banking principles.

Internal audit activities shall be performed in an objective and independent manner exercising due professional care by adequate number of auditors. Internal auditors of a bank may conduct internal auditing activities in the subsidiaries subject to consolidation. (Banking Law no.5411, 2013, pp.44-45), https://www.bddk.org.tr/websitesi/english/Legislation/14905banking_law_december_2013.pdf

Increasing importance of the risk management function at the banking sector has caused changes in organizational structures and internal auditing systems. Risk-based internal auditing is a new and modern internal auditing system that results in a change in the traditional internal auditing system. It is different from the traditional internal auditing system in terms of organizational structure and the audit processes used.

"Risk-Based Internal Auditing System" runs its operations with a tripartite structure composed of the following which reports to the bank's audit committee;

1. Internal Control Department,

2. Board of Auditors,

3. Risk Management Department. (Aslan, 2003, p.121)

Boards of Directors of banks establish audit committees for assistance of fulfillment by the board of directors of its duties related to audit and oversight. The audit committee is composed of at least two members.

The audit committee is required to get reports concerning performance of its duties from the internal control, inspection board, risk management center and independent audit agencies. In case there is a negative impact upon continuity and reliable maintenance of bank's operations or nonconformities with the legislations and internal regulations, it needs to be reported to board of directors. The committee is obliged to report results in a reliable way to the Board of Directors not less than every six month. These reports are related to committee's operations, opinions regarding

measures that need to be taken at bank, practices that need to be analyzed and important issues related to maintaining operations of the bank. (Banking Law, art. 24)

4.4.1 Risk-Based Audit

An effective internal audit system is implemented based on the risk evaluations of the internal audit unit. Risk evaluations in internal audit are procedures which are carried out by the internal audit unit to identify areas of priority in audit studies, the details to be taken into account and the frequency of audits based on the risks which the bank is exposed to and the controls relating thereto.

In order for risk evaluations to be carried out every year:

- All transactions, product varieties, offered services and duties are defined.

- Activities carried out within the scope of defined transactions, products varieties, services and duties and the provisions of the Law and other relevant legislations relating thereto are identified.

- Important business units and products as well as the operational and control risks related are determined, and documents regarding the structure of risk management and internal control system are identified.

- For the evaluation of operational and control risks related to important business units and products and the determination of degrees of importance, risk measurement and rating systems are used.

The evaluation of operational and control risks related to important business units and products and the determination of degrees of importance are carried out with the help of a matrix to cover each consolidated subsidiary. In the risk evaluation to be carried out by the internal audit unit, the risk compositions carried by the bank have to be

monitored and evaluated in terms of the areas of activity specified in the matrix as a minimum requirement.

Risk evaluations regarding units and activities are carried out jointly with unit managers. In risk evaluations, the opinions of the internal control and risk management units are also consulted. The final decision regarding risk evaluations is the responsibility of the internal audit unit. (The Regulation on Internal Systems of Banks and Evaluation Process of Internal Capital Adequacy, art. 26)

4.4.2 Objectives of Internal Auditing System in Banks

The main purposes of the internal auditing system in banks are effective and efficient use of bank's resources and prevention of possible losses. With the internal audit function, it is intended that personal interests of the employees should not take precedence over the bank's interests and employees should work in unity towards the objectives of the bank. Also, the internal audit function and internal auditors fulfilling such function are important elements of the control environment and they help achieve control objectives. (Yurtsever, 2003, p.52)

According to the regulation, "the purpose of the internal audit system is to provide assurance to the top management that the banking activities are carried out in accordance with the Law, the relevant legislation and the internal strategies, policies, principles and targets, and the internal control and risk management systems are effective and sufficient.". (The Regulation on Internal Systems of Banks and Evaluation Process of Internal Capital Adequacy, art. 21)

4.4.3 Fundamental Control Areas of Internal Audit

Areas that need to be controlled during the internal audit are addressed as main headings.

Control of transactions regarding execution of bank activities

Transactions related to execution of bank activities constitute operational activities. Controls regarding operational activities are intended to guarantee efficiency and effectiveness of operations.

Control of communication channels and information systems

Through the control of the bank's communication channels and information systems, it is intended that information generated within the bank is reliable, complete, traceable, consistent and capable of meeting the requirements in terms of format and nature, and timely accessible by the relevant units and personnel.

Control of financial reporting systems

The control of financial reporting systems aims to ensure integrity and reliability of accounting and financial reporting systems.

Compliance controls

Through compliance controls, it is intended to assure compliance of all activities and transactions which are realized and planned to be realized by the bank with the Law, the relevant legislation, the bank's internal policies, rules and banking customs. It is ensured that the bank personnel are informed about the changes in the Law, other relevant legislation, internal policies and rules as soon as possible. (The Regulation on Internal Systems of Banks and Evaluation Process of Internal Capital Adequacy Assessment, articles 15, 16, 17 and 18)

CHAPTER 5

CREATING RISK MATRIX FOR AUDIT PLANNING OF A BANK

This section includes creating risk-based internal audit matrix by considering operation mechanisms related to branch audits of a bank. The points to be taken into consideration during audits are also assessed in this section within the scope of the risk-based internal audit approach.

5.1 INTERNAL AUDIT METHODOLOGY

The internal audit activities in the banks are pursued on the basis of risk assessment performed by Board of Auditors. It is pursued in order to ensure an efficient and productive use by directing internal audit resources to more risky and priority areas with an analytical approach in the evaluation of the bank's activities.

Risk matrixes are issued in compliance with the “The Regulation on Internal Systems of Banks and Evaluation Process of Internal Capital Adequacy Assessment of Board

of Auditors" related to the determination of fields to be prioritized for audit studies, details to be taken into consideration and audit frequency.

Residual risk of audit is calculated over risk values found by using the risk model developed for branch inspections, and prioritization of audit field is made according to this residual risk value.

According to the Internal Audit Methodology; it is required to audit the fields that are considered to be more risky as a result of the risk assessments, more frequently compared to the others.

5.2 AUDIT OBJECTIVE AND BRIEF RISK ASSESSMENT

It is aimed to audit corporate and retail loans, governance and control environment, compliance issues and operational activities of the branch within the audit period.

Branch audit plan has been formed as a result of the risk assessment which takes into account credit risk, operational risk and control risk factors. Related legislations are; Banking Law and related regulations, Prevention of Laundering Proceeds of Crime Law and other related law and regulations.

5.3 RISK ASSESSMENT SYSTEM

For the creation of risk matrix related to branch audits, coefficients are calculated for credit risks, operational risks and control risks for each branch based on credit risk factors, operational risk factors and control risk factors. In the risk matrix, fifteen risk factors (six credit risk factors, five operational risk factors and four control risk factors) affecting the branch activities of the banks are used.

As a result of the multiplication of these coefficients calculated for risks, by ratios determined in risk portfolios; credit risk level, operational risk level and control risk level are found for each branch.

"Materiality" is evaluated based on professional experience. It is based on control weaknesses and shows that mistakes, negligence, contrariety against procedures and unlawful acts might effect reporting of financial data, safe and uninterrupted service at banks.

Proportional distribution of risk factors which determine credit risk level, operational risk level and control risk level are also evaluated based on materiality criteria.

“Residual Credit Risk” is calculated by the proportioning of multiplication of credit risk level calculated for branch by control risk; and “Residual Operational Risk” is calculated by the proportioning of multiplication of operational risk level by control risk.

For the general risk calculation of branch audit field, credit risk is considered 60% and operational risk is considered 40%. Accordingly, “RESIDUAL RISK” is calculated as a result of the addition of 60% of residual credit risk to 40% of residual operational risk.

Upon calculation of residual risk, risk level of each branch is found and prioritization to be included in annual audit plan is assessed accordingly. For the creation of annual audit plan, risk level as well as audit budget are the determinants.

The “residual risk” is calculated as a value between 0 and 5.

5.3.1 Credit Risk Factors and Calculation of Credit Risk Level

The credit risk factors can be summarized under the following 6 headings.

5.3.1.1 Total Credit Portfolio Size (million TRY)

It indicates credit risk figure of branch as of year-end. Its ratio among credit risks is 40%.

5.3.1.2 Close Monitoring Loan Ratio

It is the rate of risks under close monitoring to total outstanding loans as of year-end. Its ratio among credit risks is 15%.

5.3.1.3 Non-Performing Loan Ratio

It is the rate of non-performing loans to total outstanding loans as of year-end. Its ratio among credit risks is 15%.

5.3.1.4 Number of Investigations Related to Credit Transactions

Investigations conducted during the year related to credits are taken into consideration. Its ratio among credit risks is 10%.

5.3.1.5 Risk Point of Board of Auditors

Previous audit points of branches are recorded. For the new branches where an audit has not been conducted yet, an average of 75 points are taken into consideration. Its ratio among credit risks is 10%.

5.3.1.6 Bad Cheque Ratios

Bad cheque ratios recorded by a branch during the year are taken into consideration. Its ratio among credit risks is 10%.

5.3.1.7 Calculation of Credit Risk Level

Related to the above-mentioned 6 credit risk factors, coefficients from 1 to 5 are determined in proportion to figures of branches.

Credit risk level for each branch is calculated by multiplying coefficients calculated for credit risk factors by percentage ratios previously determined for credit risks.

For example; proportional distribution and credit risk based on credit risk factors for Ankara branch, which has a high risk level is like the following:

BRANCH NAME	CREDIT RISK FACTORS						CREDIT RISKS						RISK LEVEL
							40%	15%	15%	10%	10%	10%	
	Total Credit Portfolio Size (million TRY)	Close Monitoring Loan Ratio	Non-Performing Loan Ratio	Number of Investigations Related to Credit Transactions	Risk Point of Board of Auditors	Bad Cheque Ratios	Total Credit Portfolio Size (million TRY)	Close Monitoring Loan Ratio	Non-Performing Loan Ratio	Number of Investigations Related to Credit Transactions	Risk Point of Board of Auditors	Bad Cheque Ratios	CREDIT RISK LEVEL
ANKARA	428.7	0.029	0.112	1	63	0.09	5	5	5	2	3	5	4.50

Proportional distribution in credit risk factors which defines credit risk level is determined according to the "materiality" criteria mentioned in internal auditing methodology.

Credit Risk Factors	Proportional Distribution
Total Credit Portfolio Size (million TRY)	40%
Close Monitoring Loan Ratio	15%
Non-Performing Loan Ratio	15%
Number of Investigations Related to Credit Transactions	10%
Risk Point of Board of Auditors	10%
Bad Cheque Ratios	10%

The ranges of coefficients related to credit risks are determined according to the tables below:

Coefficients	Total Credit Portfolio Size (Million TRY)
1	0 - <50
2	50 - <100
3	100 - <150
4	150 - <250
5	≥ 250

Coefficients	Close Monitoring Loan Ratio
1	0 - <0.001
2	0.001 - <0.0025
3	0.0025 - <0.006
4	0.006 - <0.01
5	≥ 0.01

Coefficients	Non-Performing Loan Ratio
1	0 - <0.01
2	0.01 - <0.03
3	0.03 - <0.06

4	0.06 - <0.09
5	≥ 0.09

Coefficients	Number of Investigations Related to Credit Transactions
1	0
2	1
3	2
4	3
5	≥ 4

Coefficients	Risk Point of Board of Directors
1	0 - <40
2	40 - <60
3	60 - <75
4	75 - <90
5	≥ 90

Coefficients	Bad Cheque Ratios
1	0 - <0.02
2	0.02 - <0.03
3	0.03 - <0.04
4	0.04 - <0.06
5	≥ 0.06

Credit risk level for Ankara Branch is based on multiplication of coefficients calculated for credit risks by ratios determined in risk portfolios.

Total Credit Portfolio Size (million TRY): 5 x 40% = 2

Close Monitoring Loan Ratio: 5 x 15% = 0.75

Non-Performing Loan Ratio: 5 x 15% = 0.75

Number of Investigations Related to Credit Transactions: 2 x 10% = 0.20

Risk Point of Board of Auditors: 3 x 10% = 0.30

Bad Cheque Ratios: 5 x 10% = 0.50

CREDIT RISK LEVEL: 2 + 0.75 + 0.75 + 0.2 + 0.3 + 0.5 = 4.50

5.3.2 Operational Risk Factors and Calculation of Operational Risk Level

The operational risk factors can be classified under 5 headings.

5.3.2.1 Annual Average Cash Transaction Volume per Operation Personnel

It is calculated by dividing total cash balance by number of operation personnel as of year-end. Its ratio among operational risks is 30%.

5.3.2.2 Annual EFT (Electronic Fund Transfer) and Transfer Transaction Volume per Operation Personnel

It is found by dividing total outgoing EFT and transfer transactions that occurred during the year by number of branch's operation personnel. Its ratio among operational risks is 30%.

5.3.2.3 Number of Investigations Related to Operational Transactions

Investigations conducted during the year related to operational transactions are taken into consideration. Its ratio among operational risks is 15%.

5.3.2.4 Number of Expired Discrepancies

Number of discrepancies included in expired discrepancies report and of discrepancies belonging to branch is taken into consideration. Its ratio among operational risks is 10%.

5.3.2.5 Internal Control Department Risk Point

Last control point obtained by branch during controls conducted by the Internal Control Department is taken into consideration. Its ratio among operational risks is 15%.

5.3.2.6 Calculation of Operational Risk Level

Related to the above-mentioned 5 operational risk factors, coefficients from 1 to 5 are created in proportion to figures of branches.

Operational risk level for each branch is calculated by multiplying coefficients calculated for operational risk factors by percentage ratios previously determined for operational risks.

Operational Risk Factors	Proportional Distribution
Annual Average Cash Transaction Volume per Operation Personnel	30%
Annual EFT (Electronic Fund Transfer) and Transfer Transaction Volume per Operation Personnel	30%
Number of Investigations Related to Operational Transactions	15%
Number of Expired Discrepancies	10%
Internal Control Department Risk Point	15%

5.3.3 Control Risk Factors and Calculation of Control Risk Level

The control risk factors are gathered under 4 headings.

5.3.3.1 Surveillance of Management

A point from 1 to 5 is given by considering branch manager's efforts in terms of controlling branch transactions and their compliance with legislation, announcements and circulars. This value is determined according to the opinion of the auditor regarding the level of risk. Its ratio among control risks is 40%.

5.3.3.2 Efficiency and Adequacy of Personnel

It is found by proportioning total sector experience of manager and personnel having titles below manager to number of personnel. Its ratio among control risks is 30%.

5.3.3.3 Date of Last Audit

Time of last audit conducted in branch is taken into consideration. Its ratio among control risks is 15%.

5.3.3.4 Ratio of Actions Taken against Audit Findings

This ratio is calculated by considering number of findings resolved and its ratio to total findings which are determined as a result of finding monitoring studies conducted after audits. Its ratio among control risks is 15%.

5.3.3.5 Calculation of Control Risk Level

Related to the above-mentioned 4 control risk factors, coefficients from 1 to 5 are created in proportion to figures of branches.

Control risk level for each branch is calculated by multiplying coefficients calculated for control risk factors by percentage ratios previously determined for control risks.

Control Risk Factors	Proportional Distribution
Surveillance of Management	40%
Efficiency and Adequacy of Personnel	30%
Date of Last Audit	15%

Ratio of Actions Taken against Audit Findings	15%

5.3.4 Calculation of Residual Risk

Residual risk calculation for Ankara Branch which has a high risk level is like the following:

BRANCH NAME	RISK LEVELS			RESIDUAL RISK		RESIDUAL RISK	
	CREDIT RISK LEVEL	OPERATIONAL RISK LEVEL	CONTROL RISK LEVEL	RESIDUAL CREDIT RISK	RESIDUAL OPERATIONAL RISK		
ANKARA	4.50	3.80	4.15	3.74	3.15	**3.50**	High

"Residual Credit Risk" for Ankara Branch is calculated by multiplying the credit risk level calculated for branch by control risk and "Residual Operational Risk" is calculated by multiplying operational risk level by control risk. The results (residual credit risk and residual operational risk) are divided by 5 for re-scaling after multiplication.

"RESIDUAL RISK" for Ankara Branch is calculated by adding 60% of residual credit risk and 40% of residual operational risk.

Residual Credit Risk: (4.50 x 4.15) / 5 = 3.74

Residual Operational Risk: (3.80 x 4.15) / 5= 3.15

RESIDUAL RISK: (3.74 x 60%) + (3.15 x 40%) = 3.50

5.4 PREPARATION OF RISK MATRIX

In the previous section of this study, the calculation method of residual risk was explained in details. Related to the creation of annual audit plan for branches, risk level and audit budget are determinants. Risk level of a branch is determined by its residual risk point.

As mentioned previously, the "residual risk" to be calculated for the branches is determined on a scale from 0 to 5 and depending on risk assessments, audit period for the branches is applied for maximum 3 years.

The following table shows the risk level to be determined according to branch residual risk and the audit frequency.

RESIDUAL RISK	MINIMUM	MAXIMUM	AUDIT FREQUENCY
High	3.50	5.00	Once a Year
Moderate	2.00	3.49	Once in 2 Years
Low	0.00	1.99	Once in 3 Years

The risk matrix will be created for the annual audit plan of a bank which is assumed to have 100 branches. It is also assumed that there are 5 inspectors in the branch audit team and it is assumed that they have to audit 30 branches in year 2017.

Each bank inspector will conduct 6 branch audits during the year and the duration of each branch audit will be 30 working days. It is limited to 6 branch audits per inspector due to considerations for time spent at holidays, trainings and investigations.

According to the risk matrix created, 4 branches out of 100 branches have been calculated as having high risk, 19 of them having moderate risk and 77 of them having low risk. All of the 4 high risk branches have been included in the annual audit plan. Considering also the last audit dates of moderate and low risk branches, 10

moderate risk branches and 16 low risk branches have been included in the annual audit plan. The elapsed time between the last audit dates of the branches with moderate and low risk levels are effected into the audit plan relating branches.

Thus, the risk matrix has been created by considering all of the credit, operational and control risk factors, and the branch audit planning of a bank has been prepared within the scope of the risk-based internal audit approach.

CONCLUSION

With the developments in the economic and social life, capital flows and transaction volumes have increased. These changes resulted in operations having more risks and it became a necessity to prescribe, determine and mitigate the potential risks. As the businesses became more open to risks, the assessment and management of these risks led to the application of various methods.

In recent years, the goals and expected benefits in relation to audit changed. Today, the audit is not conducted only to examine or question but also to focus on solution, produce solution or assist the audited entity in producing the solution. At this point, a shift occurred from the methods only focusing on the systems, policies and operations to the risk-based internal audit approach focusing on risks.

In the past, internal audit and risk management processes were considered independently whereas now they are regarded as concepts interacting with and overlapping on each other and using the outputs derived by each of them. Therefore, the internal audit units of many businesses adopt the risk-based internal audit approach and develop their internal audit plans according to this framework. Internal audit is defined as all studies including the independent and objective assurance and consultancy services conducted to increase the value of the entity and ensure its efficiency within the scope of the enterprise risk management.

Risk-based internal audit is the examination of the business flows and systems with an approach that provides saving in time and cost, aims at developing measures related to risks before they occur.

In risk-based internal audit, first of all, risk status is determined and the issues such as scope, timing of audit operations and allocation of the resources are formed based on risk status. In this sense, the aim is to determine the transaction processes to be audited and to allocate the audit resources according to the risk levels of operations.

The most important way to protect the banking industry against a possible crisis is to implement a robust regulatory system and an effective audit system. In addition to independent audit, the mandatory audit of the banks is conducted by the auditors of BRSA (Banking Regulation and Supervision Agency) and also each bank has its internal auditors for auditing its operations. Risk-based internal audit shall mitigate the fragility of the system and ensure a healthier financial structure for the bank.

Adoption of risk-based internal audit approach creates a positive effect on operations of entities. In this sense, not only the effective and efficient use of the resources are realized but also the risks which are likely to be encountered by the bank are minimized or eliminated by employing various methods due to the audit operations focused on the most risky points.

The most important phase of the risk-based internal audit is to evaluate the risks. It is not proper to consider the risk evaluation efforts as a single activity. It is rather a process incorporating definition, analysis and measurement of the risks in terms of their effects and likelihoods followed by establishment of risk matrix by prioritizing the risks.

In this study, a risk matrix was created for determining the top priority areas and the frequency of internal audit work taking into account The Regulation on Internal Systems of Banks and Evaluation Process of Internal Capital Adequacy.

When forming the risk matrix related to the internal audit of bank branches, credit risk factors, operational risk factors and control risk factors were evaluated and for each branch, coefficients for credit risk, operational risk and control risk were determined. The coefficients were multiplied by percentage ratios determined in risk portfolios to calculate credit risk level, operational risk level and control risk level for each branch.

Proportional distribution of risk factors which were used to calculate credit risk level, operational risk level and control risk level were determined according to the

materiality criteria. The materiality criteria is related to safe and uninterrupted service at banks and is evaluated based on professional experience.

The factors used in determining credit risk levels and their weights are Total Credit Portfolio Size (million TRY) (40%), Close Monitoring Loan Ratio (15%), Non-Performing Loan Ratio (15%), Number of Investigations Related to Credit Transactions (10%), Risk Point of Board of Auditors (10%) and Bad Cheque Ratios (10%).

The factors used in determining operational risk levels and their weights are Annual Average Cash Transaction Volume per Operation Personnel (30%), Annual EFT (Electronic Fund Transfer) and Transfer Transaction Volume per Operation Personnel (30%), Number of Investigations Related to Operational Transactions (15%), Number of Expired Discrepancies (10%) and Internal Control Department Risk Point (15%).

The factors used in determining control risk levels and their weights are Surveillance of Management (40%), Efficiency and Adequacy of Personnel (30%), Date of Last Audit (15%) and Ratio of Actions Taken against Audit Findings (15%).

Credit risk level was multiplied by control risk to find “Residual Credit Risk” and operational risk level was multiplied by control risk to find “Residual Operational Risk”. Finally, “Residual Risk” for a branch was calculated as the sum of 60% of residual credit risk and 40% of residual operational risk. 60% weight of credit risk was based on materiality concept taking into account the losses of banks due to credit risk and was determined using professional judgement and experience.

By the help of the risk model created for the audit plan of branches, the calculated risk levels were used to determine the residual risk of audit field. According to the residual risk, the prioritization and audit frequency of the branches were effectively set.

According to the risk matrix created, 4 branches out of 100 branches have been calculated as having high risk, 19 of them having moderate risk and 77 of them having low risk. All of the high risk branches have been included in the annual audit plan. Taking into account the last audit dates of moderate and low risk branches, in addition to 4 high risk branches, 10 moderate risk branches and 16 low risk branches have been included in the annual audit plan.

In summary, the risk levels of the branch operations in the banks were evaluated using a risk matrix based on risk-based internal audit approach. The risks were evaluated and weights were assigned to fifteen risk factors employed in the study and the branches having higher risks were included in the annual audit plan.

REFERENCES

Abdioğlu, H., 2008. İç Denetim Alanında Mesleki Yetkinliklerin Güçlendirilmesi Arayışları ve İngiltere-İrlanda İç Denetçiler Enstitüsünün Yetkinlik Tanımlamaları. Sayıştay Dergisi, 68, p.91.

ACCA, COSO Enterprise Risk Management Framework, The ERM Model, May 2017, para.1-2, http://www.accaglobal.com/uk/en/student/exam-support-resources/professional-exams-study-resources/p1/technical-articles/coso-enterprise-risk-management-framework-part-1.html

Adiloğlu, B., 2011. İç Denetim Süreci ve Kontrol Prosedürleri. Türkmen Kitabevi, p.67.

Akarkarasu, N., 2000. Halka Açık Şirketlerde İç Denetim ve Denetim Kurullarının Etkinleştirilmesi İçin Öneriler, Yeterlilik Etüdü. SPK Denetleme Dairesi, p.16.

Akgül, B. A., 2000. Türk Denetim Kurumları. Türkmen Kitabevi, pp.13-68.

Aksoy, T., 2006. Tüm Yönleriyle Denetim. Yetkin Yayınları, pp.47-1479.

Alptürk, E., 2008. İç Denetim Rehberi. Maliye ve Hukuk Yayınları, p.22.

Aslan, B., 2010. Bir Yönetim Fonksiyonu Olarak İç Denetim. Sayıştay Dergisi, 77, p. 82.

Aslan, Ö. & Küçükaksoy, İ., 2006. Finansal Gelişme ve Ekonomik Büyüme İlişkisi: Türkiye Ekonomisi Üzerine Ekonometrik Bir Uygulama. İstanbul Üniversitesi İktisat Fakültesi Ekonometri ve İstatistik Dergisi, 4, pp.8-13.

Aslan, S., 2003. Türk Bankacılık Sektöründe İç Denetim. Avcıol Basım-Yayın, p.121.

Bank for International Settlements (BIS), 2012. Basel Committee on Banking Supervision (Core Principles for Effective Banking Supervision), pp.1-13.

Banking Regulation and Supervision Agency (BRSA), 2005. 5411 Sayılı Bankacılık Kanunu. Resmi Gazete, Sayı: 25983, art.24.

Banking Regulation and Supervision Agency (BRSA), 2006. Bankalarda Bağımsız Denetim Gerçekleştirecek Kuruluşların Yetkilendirilmesi ve Faaliyetleri Hakkında Yönetmelik. Resmi Gazete, Sayı: 26333, p.3, http://www.bddk.org.tr/WebSitesi/turkce/Mevzuat/Bankacilik_Kanununa_Iliskin_Duzenlemeler/140131677bagimsiz_denetim_islenmis_nihai_webe_basbakanliktan_sonra.pdf

Banking Regulation and Supervision Agency (BRSA), 2013. Banking Law no.5411, 3, pp.44-45, https://www.bddk.org.tr/websitesi/english/Legislation/14905banking_law_december_2013.pdf

Banking Regulation and Supervision Agency (BRSA), 2014. Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik. Resmi Gazete, Sayı: 28896, p.10,

http://www.bddk.org.tr/WebSitesi/turkce/Mevzuat/Bankacilik_Kanununa_Iliskin_Duzenlemeler/9486bsd_yonetmeligi.pdf

Banking Regulation and Supervision Agency (BRSA), 2014. Bankaların İç sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik, Resmi Gazete, Sayı: 29057, art.15-26.

Benli, V. F. & Celayir, D., 2014. Risk Based Internal Auditing and Risk Assessment Process. European Journal of Accounting Auditing and Finance Research, 2(7), pp.1-16.

Bolgün, K.E. & Akçay, M.B, 2003. Risk Yönetimi. Skala Yayıncılık, p.414.

Bozkurt, C., 2010. Risk, Kurumsal Risk Yönetimi ve İç Denetim. Denetişim Dergisi, pp.22-26.

Ceylan, A. & Korkmaz, T., 2008. İşletmelerde Finansal Yönetim. Ekin Yayınevi, 10, p.494.

Derici, O. & Tüysüz, Z. & Sarı, A., 2007. Kurumsal Risk Yönetimi ve Sayıştay Uygulaması. Sayıştay Dergisi, 65, pp.153-154.

Dornberger, K. & Oberlehner, S. & Zadrazil, N., 2014. Challenges in Implementing Enterprise Risk Management. Journal of Finance and Risk Perspectives, (3)3, pp.3-4.

Erdoğan, M., 2006. Denetim Kavramsal ve Teknolojik Yapı. Maliye ve Hukuk Yayınları, 3, p.5.

Ergüden, A.E. Risk Odaklı İç Denetim Modellemesi. Tokkder, http://tokkder.org/tokkder-dergi/1080

Eşkazan, A.R., 2005. Risk Odaklı İç Denetim Planlaması. Türkiye İç Denetim Enstitüsü İç Denetim Dergisi, 11, p.33.

Fraser, J. & Lindsay, H., 2005. Yönetim Kurullarının İç Denetim Hakkında Sorması Gereken 20 Soru. İç Denetim Dergisi, 11, p.21.

Göğüş, E.H.S., 2012. Risk Odaklı İç Denetimde Risklerin Saptanması ve Değerlendirilmesi. Türkmen Kitabevi, pp.47-68.

Griffiths, D., 2006. Risk Based Internal Auditing –Three Vıews on Implemantation. pp.1-2, http://www.internalaudit.biz/files/implementation/rbiaimplementing.pdf

Griffiths, P., 2005. Risk-Based Auditing. Gower Publishing Limited, pp.5-117.

Gürbüz, H., 1995. Muhasebe Denetimi. Bilim ve Teknik Yayınları, p.50.

Güredin, E., 2000. Denetim. Beta Yayınevi, 10, p.9.

Institute of Internal Auditors (IIA), 2015. What is Internal Audit?, https://www.iia.org.uk/about-us/what-is-internal-audit/#what

International Standard on Auditing (ISA) 200, 2010. http://www.ifac.org/system/files/downloads/a008-2010-iaasb-handbook-isa-200.pdf

Karanfiloğlu, A.Y., 1999. Muhasebe Denetimi Kavram İlke ve Yöntemleri. Sayıştay Dergisi, 35, p.30.
Kaval, H., 2003. Muhasebe Denetimi. Akademik Denetim Danışmanlık ve YMM A.Ş., p.25.

Kepekçi, C., 2000. Bağımsız Denetim. Avcıol Basım Yayın, 4, pp.4-123.

Keskin, D.A., 2006. İç Kontrol Sistemi Kontrol Öz Değerlendirme. Beta Yayıncılık, p.16.
Kır, H., 2010. Stratejik Denetim ve Denetimde Risk Odaklılık. Denetişim Dergisi, 4, pp.53-54.

Kishalı, Y. & Pehlivanlı, D., 2006. Risk Odaklı İç Denetim ve İMKB Uygulaması. Muhasebe ve Finansman Dergisi, 30, pp.75-79.

Kurnaz, N. & Çetinoğlu T., 2010. İç Denetim Güncel Yaklaşımlar. Umuttepe Yayınları, pp.11-153.

Kurtoğlu, Ç., 2004. Kurum Çapında Risk Yönetiminde İç Denetimin Rolü. İç Denetim Dergisi, p.22.

Merna, T. & Al-Thani, F.F., 2005. Corporate Risk Management an Organizational Perspective. John Willey&Sons Ltd., pp.9-38.

Moeller, R.R., 2005. Brink's Modern Internal Auditing. John Wiley&Sons Inc., 6, pp.3-405.

Moeller, R.R., 2007. COSO Enterprise Risk Management-Understanding the New Integrated ERM Framework. John Wiley&Sons Inc., p.22-248.

Özaydın, M.E., 2010. Riskin Tanımlanması ve Kamu İdarelerinde Nitelikli İç Denetim Faaliyetinin Yürütülmesini Engelleyen Riskler. Denetişim Dergisi, 4, p.32.

Özbek, Ç., 2012. İç Denetim Kurumsal Yönetim Risk Yönetimi İç Kontrol. Türkiye İç Denetim Enstitüsü Yayınları, (3)1, pp.6-49.

Özbek, Ç., 2012. İç Denetim Kurumsal Yönetim Risk Yönetimi İç Kontrol. Türkiye İç Denetim Enstitüsü Yayınları, (3)2, pp.807-1013.

Özoğlu, B. & Mercan, C. & Çakıroğlu, S., 2010. Bir Güvence ve Danışmanlık Hizmeti İç Denetim. İ.B.B. İç Denetim Birimi Başkanlığı Yayınları, 1, pp.29-57.

Pehlivanlı, D., 2010. Modern İç Denetim. Beta Yayınları, pp.121-137.

Price Waterhouse Coopers, 2006. Her Yönüyle Kurumsal Risk Yönetimi. İnfomag Yayıncılık, p.4.

Probability and Impact Matrix, Manick, 14 February 2012, para.2-4, http://www.justgetpmp.com/2012/02/probability-and-impact-matrix.html

PwC Business School, 2009. Sürdürülebilir Kurumsal Risk Yönetimi Yaklaşımının Oluşturulması. VIII. Çözüm Ortaklığı Platformu, p.11.

Ratliff, R.L. & Reding, K.F., 2002. Introduction to Auditing: Logic, Principles and Techniques. IIA Publications, p.16.
Roth, J. & Espersen, D., 2002. Riskin Sınıflandırılması, İç Denetim Dergisi, 4, p.18.

Saltık, N., 2007. İç Kontrol Standartları. T.C.Maliye Bakanlığı Bütçe ve Kontrol Genel Müdürlüğü, pp.21-22.

Sawyer, L.B. & Dittenhofer, M.A., 2002. Sawyer's Internal Auditing. IIA Publications, 5, p.6.

Spencer Pickett, K.H., 2003. The International Auditing Handbook. Wiley, 2, pp.10-605.

Spencer Pickett, K.H., 2004. The Internal Auditor at Work: A Practical Guide to Everyday Challenges. John Wiley&Sons, pp.159-160.

Spencer Pickett, K.H., 2006. Audit Planning: A Risk Based Approach. John Wiley&Sons, pp.28-176.

The European Confederation of Institutes of Internal Auditing (ECIIA). T.C Kültür ve Turizm Bakanlığı-İç Denetim Birimi Başkanlığı, Mesleki Kuruluşlar, http://icdenetim.kultur.gov.tr/TR,46902/mesleki-kuruluslar.html

The European Confederation of Institutes of Internal Auditing (ECIIA). What is Internal Auditing?, http://www.eciia.eu/what-we-do/what-is-internal-auditing/

The Institute of Internal Auditing–Turkey, 2015. Global Partner of Excellence in the Profession: The Institute of Internal Auditing-Turkey, https://www.tide.org.tr/uploads/brosurrbaski.pdf

The Institute of Internal Auditors (THEIIA), 2012. International Standards for The Professional Practice of Internal Auditing, pp.3-18.

https://na.theiia.org/standards-guidance/Public%20Documents/IPPF%202013%20English.pdf

The Institute of Internal Auditors-UK&Ireland, 2003. Position Statement-Risk Based Internal Auditing, p.1.

Toroslu, M.V., 2012. Yeni Türk Ticaret Kanunu Kapsamında Finansal Tablolar Denetimi. Seçkin Yayınevi, p.70.

Turkish Language Society (TDK), 01.12.2016.

Türkiye İç Denetim Enstitüsü, Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi, Türkiye İç Denetim Enstitüsü Yayınları, 2004. Lebib Yalkın Yayınları, 3, p.308.

Ulusoy, Y., 2007. Bağımsız Dış Denetim. Seçkin Yayınevi, p.102.

Yılmaz, H.G., 2004. Yeminli Mali Müşavirlerin Müşterek ve Müteselsil Sorumluluklarının Temel İnsan Hakları, Avrupa Birliği Hukuku, Anayasa Hukuku ve Borçlar Hukuku Yönünden Değerlendirilmesi. Yeminli Mali Müşavirler Odası Yayını, p.22.

Yurtsever, G., 2003. Türk Bankacılığının Kontrol ve Denetim Yapısı İçinde İç Kontrol Merkezinin Yeri. Active Finans ve Bankacılık Dergisi, 33, p.52.

Appendix

Appendix-1

BRANCH NAME	CREDIT RISK FACTORS						OPERATIONAL RISK FACTORS					CONTROL RISK FACTORS			
	Total Credit Portfolio Size (million TRY)	Close Monitoring Loan Ratio	Non-Performing Loan Ratio	Number of Investigations Related to Credit Transactions	Risk Point of Board of Auditors	Bad Cheque Ratios	Annual Average Cash Transaction Volume per Operation Personnel (million TRY)	Annual EFT (Electronic Fund Transfer) and Transfer Transaction Volume per Operation Personnel	Number of Investigations Related to Operational Transactions	Number of Expired Discrepancies	Internal Control Department Risk Point	Surveillance of Management	Efficiency and Adequacy of Personnel	Date of Last Audit	Ratio of Actions Taken Against Audit Findings
ADANA	380.0	0.004	0.036	0	64	0.09	107.61	1251	1	124	24.27	3	7.71	9/26/2014	0.822
ADIYAMAN	198.0	0.002	0.024	0	69	0.03	82.02	997	0	71	30.11	2	6.51	1/11/2015	0.566
AFYONKARAHİSAR	152.5	0.018	0.014	0	72	0.01	78.63	733	0	28	17.05	1	7.02	5/8/2014	0.652
AĞRI	178.3	0.022	0.012	1	81	0.00	57.98	1145	0	17	16.62	2	5.37	8/18/2014	0.887
AKSARAY	92.9	0.003	0.029	0	75	0.04	37.12	792	0	34	18.84	3	6.19	7/25/2016	0.779
AMASYA	155.6	0.011	0.087	0	72	0.08	69.38	829	0	55	28.96	3	5.42	4/12/2014	0.674
ANKARA	428.7	0.029	0.112	1	63	0.09	201.26	1236	1	136	19.27	4	3.21	2/17/2016	0.662
ANKARA BALGAT	219.5	0.001	0.020	0	74	0.04	108.12	1123	0	38	24.96	2	7.25	5/18/2016	0.441
ANKARA ÇANKAYA	213.4	0.002	0.051	0	84	0.20	96.62	994	0	74	15.53	2	5.89	12/3/2015	0.900
ANKARA ETLİK	166.9	0.023	0.017	0	69	0.03	78.85	745	0	51	21.22	2	4.26	6/16/2016	0.689
ANKARA KIZILAY	202.8	0.001	0.014	0	86	0.02	101.15	672	0	26	16.25	3	7.52	3/11/2015	0.884
ANKARA ULUS	296.7	0.026	0.079	0	68	0.09	126.23	852	0	39	15.42	4	4.15	4/17/2014	0.541
ANTALYA	233.6	0.015	0.072	0	72	0.08	114.59	956	0	52	25.08	3	3.29	8/5/2015	0.713
ARDAHAN	98.7	0.008	0.092	0	71	0.00	69.53	362	1	129	22.35	1	6.23	9/15/2016	0.726
ARTVİN	115.4	0.002	0.023	0	63	0.05	51.42	663	0	64	39.61	2	3.26	3/10/2014	0.638
AYDIN	179.6	0.096	0.112	0	68	0.06	54.26	762	0	84	19.42	2	7.82	10/3/2014	0.824
BALIKESİR	128.8	0.020	0.001	0	77	0.00	56.21	456	1	17	9.25	2	6.25	11/9/2015	0.714
BARTIN	89.9	0.001	0.003	0	67	0.02	33.20	524	1	33	22.52	3	3.26	10/15/2016	0.552
BATMAN	169.9	0.010	0.078	0	72	0.05	66.23	956	0	26	14.26	3	6.08	7/12/2015	0.924
BAYBURT	123.3	0.005	0.004	1	76	0.00	49.52	773	0	51	9.51	2	5.86	8/28/2016	0.412
BİLECİK	92.3	0.002	0.039	0	64	0.01	109.56	452	0	23	29.36	2	7.12	12/22/2016	0.712
BİNGÖL	164.2	0.009	0.012	1	75	0.09	76.05	326	0	62	32.26	1	6.32	8/12/2014	0.616

BRANCH NAME	CREDIT RISK FACTORS						OPERATIONAL RISK FACTORS					CONTROL RISK FACTORS			
	Total Credit Portfolio Size (million TRY)	Close Monitoring Loan Ratio	Non-Performing Loan Ratio	Number of Investigations Related to Credit Transactions	Risk Point of Board of Auditors	Bad Cheque Ratios	Annual Average Cash Transaction Volume per Operation Personnel (million TRY)	Annual EFT (Electronic Fund Transfer) and Transfer Transaction Volume per Operation Personnel	Number of Investigations Related to Operational Transactions	Number of Expired Discrepancies	Internal Control Department Risk Point	Surveillance of Management	Efficiency and Adequacy of Personnel	Date of Last Audit	Ratio of Actions Taken Against Audit Findings
BİTLİS	189.0	0.036	0.021	0	79	0.11	52.30	224	0	12	16.20	2	4.75	4/19/2015	0.589
BOLU	178.7	0.070	0.003	0	81	0.05	102.61	714	1	26	8.96	2	5.04	6/23/2016	0.451
BURDUR	101.9	0.004	0.042	0	73	1.01	41.20	235	0	39	12.40	3	4.48	5/20/2015	0.858
BURSA	387.4	0.120	0.091	1	77	0.78	145.60	952	0	41	26.90	3	6.01	12/28/2014	0.652
ÇANAKKALE	226.5	0.003	0.013	0	84	0.06	126.80	877	1	62	19.03	2	7.12	2/15/2015	0.714
ÇANKIRI	139.9	0.008	0.002	0	76	0.02	32.90	412	0	28	32.10	2	3.97	9/22/2014	0.515
ÇORUM	201.1	0.004	0.023	0	79	0.02	62.10	741	0	56	13.89	2	5.49	1/2/2015	1.000
DENİZLİ	412.0	0.021	0.223	1	61	0.09	192.40	1231	1	105	32.90	5	4.03	1/30/2016	0.336
DİYARBAKIR	302.8	0.007	0.066	0	81	0.06	152.60	774	0	56	12.10	2	6.21	10/6/2015	0.895
DÜZCE	86.4	0.002	0.054	0	73	0.01	33.89	565	1	61	22.10	3	7.14	1/17/2014	0.652
EDİRNE	192.6	0.001	0.000	0	82	0.00	59.90	422	0	16	8.40	1	4.52	2/18/2014	1.000
ELAZIĞ	86.9	0.008	0.011	0	70	0.03	66.21	621	0	52	21.74	3	6.51	9/30/2016	0.774
ERZİNCAN	176.7	0.005	0.092	0	62	0.16	42.11	745	1	39	41.11	4	4.94	3/16/2015	0.696
ERZURUM	201.5	0.008	0.037	0	81	0.08	91.87	856	0	52	18.80	2	7.41	6/19/2014	0.720
ESKİŞEHİR	185.4	0.001	0.009	0	79	0.02	132.10	926	0	87	13.60	3	6.98	6/10/2015	0.848
GAZİANTEP	404.3	0.210	0.645	1	69	1.21	208.30	743	0	46	22.30	3	5.80	1/12/2016	0.542
GİRESUN	125.4	0.002	0.012	0	76	0.02	48.57	663	0	52	12.63	1	3.93	8/12/2016	0.478
GÜMÜŞHANE	106.6	0.004	0.026	0	62	0.01	36.50	529	0	65	19.36	2	4.51	1/29/2014	1.000
HAKKARİ	201.4	0.002	0.071	0	76	0.01	159.80	1123	1	95	36.23	3	8.14	5/26/2015	0.412
HATAY	198.7	0.003	0.003	0	80	0.05	114.52	841	0	61	14.52	2	6.22	3/28/2014	0.854
ISPARTA	223.8	0.004	0.023	1	69	0.98	152.40	884	0	73	22.62	4	5.21	9/16/2016	0.745
MERSİN	98.6	0.021	0.005	0	71	0.04	59.40	542	0	26	19.60	3	4.26	9/20/2015	0.704
IĞDIR	116.9	0.006	0.002	0	78	0.02	63.25	751	1	49	14.97	3	4.16	11/15/2014	0.852
İSTANBUL	475.6	0.009	0.021	0	84	0.07	263.50	1156	0	126	15.41	1	8.25	2/16/2016	0.745
İSTANBUL EMİNÖNÜ	399.6	0.007	0.036	0	78	0.12	206.94	994	0	96	22.13	3	3.96	8/2/2015	0.542
İSTANBUL GÜNEŞLİ	386.5	0.125	0.036	1	72	0.62	198.41	884	0	62	16.32	2	7.38	12/1/2014	0.897
İSTANBUL KADIKÖY	357.0	0.009	0.122	0	78	0.57	185.40	963	0	112	21.32	2	8.52	12/9/2015	0.789
İSTANBUL KARAKÖY	485.2	0.023	0.016	0	79	0.12	253.36	1154	0	65	16.52	2	9.42	4/25/2016	0.596

BRANCH NAME	CREDIT RISK FACTORS						OPERATIONAL RISK FACTORS					CONTROL RISK FACTORS			
	Total Credit Portfolio Size (million TRY)	Close Monitoring Loan Ratio	Non-Performing Loan Ratio	Number of Investigations Related to Credit Transactions	Risk Point of Board of Auditors	Bad Cheque Ratios	Annual Average Cash Transaction Volume per Operation Personnel (million TRY)	Annual EFT (Electronic Fund Transfer) and Transfer Transaction Volume per Operation Personnel	Number of Investigations Related to Operational Transactions	Number of Expired Discrepancies	Internal Control Department Risk Point	Surveillance of Management	Efficiency and Adequacy of Personnel	Date of Last Audit	Ratio of Actions Taken Against Audit Findings
İSTANBUL KOZYATAĞI	523.4	0.063	0.656	1	74	0.92	301.23	1665	0	126	36.52	5	2.99	1/26/2016	0.442
İSTANBUL MECİDİYEKÖY	336.5	0.056	0.123	0	79	0.36	202.15	985	0	84	19.56	2	7.26	7/15/2015	0.856
İSTANBUL OSMANBEY	401.3	0.035	0.028	0	72	0.09	256.31	1263	1	56	12.45	1	8.42	7/23/2014	0.712
İSTANBUL TAKSİM	299.7	0.004	0.026	0	81	0.02	125.63	856	0	63	16.53	2	5.38	11/16/2016	0.812
İSTANBUL ÜSKÜDAR	412.3	0.156	0.412	1	69	0.39	263.35	1052	0	84	18.52	3	4.02	2/12/2015	0.741
İSTANBUL ZEYTİNBURNU	289.5	0.042	0.021	0	76	0.12	186.52	963	1	62	29.85	2	7.45	8/12/2014	0.828
İZMİR	373.4	0.005	0.036	0	78	0.03	226.41	784	0	81	30.23	2	8.02	7/16/2016	0.622
İZMİR BORNOVA	198.9	0.009	0.026	0	80	0.05	98.56	652	0	36	16.62	2	6.32	3/15/2015	0.598
İZMİR KARABAĞLAR	176.5	0.002	0.015	0	74	0.02	101.25	856	0	44	19.57	2	6.95	10/30/2016	0.660
İZMİR KARŞIYAKA	263.1	0.071	0.019	0	72	0.06	125.69	745	0	26	22.63	3	3.26	3/27/2014	0.779
İZMİR MENEMEN	202.6	0.002	0.009	1	75	0.04	93.26	814	0	66	18.52	2	5.21	6/18/2014	0.698
KARABÜK	88.9	0.001	0.002	0	82	0.01	38.63	697	0	28	13.12	2	4.66	6/24/2015	0.701
KARAMAN	101.2	0.003	0.006	0	79	0.04	42.15	795	0	36	18.19	1	6.59	2/11/2016	1.000
KARS	92.5	0.002	0.003	0	88	0.01	57.23	556	0	28	16.62	2	8.68	12/8/2015	0.778
KASTAMONU	127.9	0.014	0.004	0	72	0.03	86.56	745	0	49	22.63	2	5.95	5/12/2014	0.668
KAYSERİ	296.5	0.102	0.075	1	70	0.16	186.52	1156	0	92	29.82	3	4.42	3/19/2016	0.801
KIRIKKALE	107.8	0.001	0.026	0	75	0.02	44.56	665	0	53	14.52	2	7.21	12/10/2014	0.741
KIRKLARELİ	92.6	0.002	0.003	0	81	0.01	25.63	598	0	39	11.23	2	7.03	2/24/2015	0.696
KIRŞEHİR	78.4	0.010	0.002	0	77	0.01	30.26	674	1	28	15.63	3	6.23	7/20/2016	0.512
KİLİS	185.6	0.008	0.096	1	69	0.48	115.60	856	0	74	19.26	3	5.96	7/12/2014	0.702
KOCAELİ	175.4	0.004	0.002	0	82	0.01	79.05	714	0	23	16.89	2	4.10	11/6/2015	0.425
KONYA	189.5	0.029	0.006	0	65	0.06	112.03	884	0	69	29.67	3	8.41	4/21/2016	0.789
KÜTAHYA	83.7	0.013	0.002	0	71	0.09	54.23	541	0	40	15.22	3	5.26	11/6/2014	0.801
MALATYA	163.3	0.007	0.032	1	67	0.26	84.11	856	0	73	39.41	3	5.84	1/3/2015	0.412
MANİSA	209.1	0.000	0.001	0	90	0.02	101.20	942	0	12	9.23	1	6.23	2/4/2014	0.811
KAHRAMANMARAŞ	221.5	0.094	0.001	0	73	0.06	98.52	1027	0	84	26.52	3	3.60	3/24/2016	0.641

BRANCH NAME	CREDIT RISK FACTORS						OPERATIONAL RISK FACTORS					CONTROL RISK FACTORS			
	Total Credit Portfolio Size (million TRY)	Close Monitoring Loan Ratio	Non-Performing Loan Ratio	Number of Investigations Related to Credit Transactions	Risk Point of Board of Auditors	Bad Cheque Ratios	Annual Average Cash Transaction Volume per Operation Personnel (million TRY)	Annual EFT (Electronic Fund Transfer) and Transfer Transaction Volume per Operation Personnel	Number of Investigations Related to Operational Transactions	Number of Expired Discrepancies	Internal Control Department Risk Point	Surveillance of Management	Efficiency and Adequacy of Personnel	Date of Last Audit	Ratio of Actions Taken Against Audit Findings
MARDİN	181.0	0.007	0.002	0	76	0.02	75.26	651	1	66	23.10	2	9.08	10/25/2015	1.000
MUĞLA	156.2	0.003	0.017	0	70	0.26	51.20	574	0	122	22.68	3	6.11	6/11/2014	0.849
MUŞ	86.6	0.005	0.001	0	72	0.05	26.60	320	0	29	18.74	3	6.23	10/3/2016	0.724
NEVŞEHİR	129.8	0.003	0.004	0	74	0.01	96.52	554	0	63	26.30	2	5.26	5/17/2015	0.559
NİĞDE	68.7	0.005	0.007	0	82	0.06	29.63	426	0	23	16.55	2	6.88	8/11/2016	0.662
ORDU	216.7	0.016	0.001	0	72	0.03	126.30	1039	0	74	14.25	2	7.12	10/20/2015	0.641
OSMANİYE	105.3	0.004	0.006	1	80	0.07	98.40	665	0	25	15.21	2	7.85	1/18/2014	0.884
RİZE	251.0	0.016	0.182	0	71	0.13	156.21	841	1	66	38.03	4	6.92	5/8/2016	0.741
SAKARYA	135.2	0.005	0.003	0	79	0.02	95.23	674	0	47	21.22	3	8.03	9/12/2015	0.875
SAMSUN	253.6	0.029	0.032	1	64	0.71	201.40	1365	1	122	36.91	4	3.21	3/1/2016	0.322
SİİRT	152.4	0.005	0.002	0	78	0.01	68.52	740	0	46	16.99	1	6.78	11/25/2014	0.819
SİNOP	136.5	0.004	0.001	0	72	0.03	86.20	863	0	69	14.22	2	6.23	8/16/2015	0.770
SİVAS	198.2	0.084	0.060	0	76	0.22	163.20	1022	0	30	15.62	2	7.91	6/9/2016	0.821
TEKİRDAĞ	85.2	0.003	0.000	0	81	0.00	32.61	554	0	74	11.40	2	5.57	9/19/2014	0.925
TOKAT	101.7	0.012	0.003	0	75	0.08	64.10	743	0	101	26.14	2	6.88	9/23/2015	0.652
TRABZON	226.9	0.016	0.005	0	70	0.01	152.10	1451	0	61	20.41	2	7.02	11/2/2016	1.000
TUNCELİ	106.2	0.003	0.006	0	69	0.05	58.41	666	0	53	17.42	2	4.98	10/28/2014	0.811
ŞANLIURFA	172.4	0.008	0.001	0	72	0.02	115.22	878	1	115	32.16	3	3.84	11/9/2015	0.674
ŞIRNAK	103.3	0.001	0.004	0	75	0.02	122.60	329	0	35	18.55	2	4.17	12/2/2016	0.652
UŞAK	154.6	0.002	0.001	0	79	0.01	198.44	1211	0	97	20.36	3	7.14	2/18/2014	0.857
VAN	193.5	0.000	0.016	1	68	0.06	206.53	845	0	74	40.15	3	4.08	4/18/2015	0.748
YALOVA	112.6	0.008	0.001	0	73	0.01	91.26	952	0	62	14.29	1	6.98	4/16/2016	0.601
YOZGAT	65.4	0.001	0.000	0	81	0.02	78.48	803	0	81	19.92	3	5.25	4/8/2014	0.812
ZONGULDAK	189.6	0.002	0.001	0	73	0.00	152.60	705	0	73	20.57	2	6.22	6/11/2015	0.791

Appendix-2

BRANCH NAME	CREDIT RISKS						OPERATIONAL RISKS					CONTROL RISKS				RISK LEVELS			RESIDUAL RISK		RESIDUAL RISK	
	40%	15%	15%	10%	10%	10%	30%	30%	15%	10 %	15%	40 %	30 %	15 %	15%							
	Total Credit Portfolio Size (million TRY)	Close Monitoring Loan Ratio	Non-Performing Loan Ratio	Number of Investigations Related to Credit Transactions	Risk Point of Board of Auditors	Bad Cheque Ratios	Annual Average Cash Transaction Volume per Operatiom Personnel (Milyon TL)	Annual EFT (Electronic Fund Transfer) and Transfer Transaction Volume per Operration Personnel	Number of Investigations Related to Operational Transactions	Number of Expired Discrepancies	Internal Control Department Risk Point	Surveillance of Management	Efficiency and Adequacy of Personnel	Date of Last Audit	Ratio of Actions Taken Against Audit Findings	CREDIT RISK LEVEL	OPERATIONAL RISK LEVEL	CONTROL RISK LEVEL	RESIDUAL CREDIT RISK	RESIDUAL OPERATIONAL RISK	RESIDUAL RISK	
ADANA	5	3	3	1	3	5	4	3	2	5	5	3	2	5	3	3,80	3,65	3,00	2,28	2,19	**2,24**	Moderate
ADIYAMAN	4	2	2	1	3	3	4	2	1	5	5	2	3	5	5	2,90	3,20	3,20	1,86	2,05	**1,93**	Low
AFYONKARAHİSAR	4	5	2	1	3	1	3	1	1	2	4	1	2	5	4	3,15	2,15	2,35	1,48	1,01	**1,29**	Low
AĞRI	4	5	2	2	2	1	3	3	1	1	4	2	4	5	2	3,15	2,65	3,05	1,92	1,62	**1,80**	Low
AKSARAY	2	3	2	1	2	4	2	1	1	2	4	3	3	1	3	2,25	1,85	2,70	1,22	1,00	**1,13**	Low
AMASYA	4	5	4	1	3	5	3	2	1	4	5	3	4	5	4	3,85	2,80	3,75	2,89	2,10	**2,57**	Moderate
ANKARA	5	5	5	2	3	5	5	3	2	5	4	4	5	3	4	4,50	3,80	4,15	3,74	3,15	**3,50**	High
ANKARA BALGAT	4	2	2	1	3	4	4	3	1	2	5	2	2	2	5	3,00	3,20	2,45	1,47	1,57	**1,51**	Low
ANKARA ÇANKAYA	4	2	3	1	2	5	4	2	1	5	4	2	4	4	2	3,15	3,05	2,90	1,83	1,77	**1,80**	Low
ANKARA ETLİK	4	5	2	1	3	3	3	1	1	4	5	2	4	2	4	3,35	2,50	2,90	1,94	1,45	**1,75**	Low
ANKARA KIZILAY	4	1	2	1	2	2	4	1	1	2	4	3	2	5	2	2,55	2,45	2,85	1,45	1,40	**1,43**	Low
ANKARA ULUS	5	5	4	1	3	5	5	2	1	2	4	4	4	5	5	4,25	3,05	4,30	3,66	2,62	**3,24**	Moderate
ANTALYA	4	5	4	1	3	5	4	2	1	4	5	3	5	5	4	3,85	3,10	4,05	3,12	2,51	**2,88**	Moderate
ARDAHAN	2	4	5	1	3	1	3	1	2	5	5	1	3	1	4	2,65	2,75	2,05	1,09	1,13	**1,10**	Low
ARTVİN	3	2	2	1	3	4	3	1	1	5	5	2	5	5	5	2,60	2,60	3,80	1,98	1,98	**1,98**	Low

BRANCH NAME	CREDIT RISKS						OPERATIONAL RISKS					CONTROL RISKS				RISK LEVELS			RESIDUAL RISK		RESIDUAL RISK	
	40%	15%	15%	10%	10%	10%	30%	30%	15%	10 %	15%	40 %	30 %	15 %	15%							
	Total Credit Portfolio Size (million TRY)	Close Monitoring Loan Ratio	Non-Performing Loan Ratio	Number of Investigations Related to Credit Transactions	Risk Point of Board of Auditors	Bad Cheque Ratios	Annual Average Cash Transaction Volume per Operatiom Personnel (Milyon TL)	Annual EFT (Electronic Fund Transfer) and Transfer Transaction Volume per Operration Personnel	Number of Investigations Related to Operational Transactions	Number of Expired Discrepancies	Internal Control Department Risk Point	Surveillance of Management	Efficiency and Adequacy of Personnel	Date of Last Audit	Ratio of Actions Taken Against Audit Findings	CREDIT RISK LEVEL	OPERATIONAL RISK LEVEL	CONTROL RISK LEVEL	RESIDUAL CREDIT RISK	RESIDUAL OPERATIONAL RISK	RESIDUAL RISK	
AYDIN	4	5	5	1	3	5	3	1	1	5	4	2	2	5	3	4,00	2,45	2,60	2,08	1,27	**1,76**	Low
BALIKESİR	3	5	1	1	2	1	3	1	2	1	2	2	3	4	4	2,50	1,90	2,90	1,45	1,10	**1,31**	Low
BARTIN	2	1	1	1	3	2	2	1	2	2	5	3	5	1	5	1,70	2,15	3,60	1,22	1,55	**1,35**	Low
BATMAN	4	5	4	1	3	4	3	2	1	2	3	3	3	5	2	3,75	2,30	3,15	2,36	1,45	**2,00**	Low
BAYBURT	3	3	1	2	2	1	2	1	1	4	2	2	4	1	5	2,30	1,75	2,90	1,33	1,02	**1,21**	Low
BİLECİK	2	2	3	1	3	1	4	1	1	2	5	2	2	1	4	2,05	2,60	2,15	0,88	1,12	**0,98**	Low
BİNGÖL	4	4	2	2	2	5	3	1	1	5	5	1	3	5	5	3,40	2,60	2,80	1,90	1,46	**1,72**	Low
BİTLİS	4	5	2	1	2	5	3	1	1	1	4	2	4	5	5	3,45	2,05	3,50	2,42	1,44	**2,02**	Moderate
BOLU	4	5	1	1	2	4	4	1	2	2	2	2	4	2	5	3,20	2,30	3,05	1,95	1,40	**1,73**	Low
BURDUR	3	3	3	1	3	5	2	1	1	2	3	3	4	5	2	3,00	1,70	3,45	2,07	1,17	**1,71**	Low
BURSA	5	5	5	2	2	5	5	2	1	3	5	3	3	5	4	4,40	3,30	3,45	3,04	2,28	**2,73**	Moderate
ÇANAKKALE	4	3	2	1	2	5	5	2	2	5	4	2	2	5	4	3,15	3,50	2,75	1,73	1,93	**1,81**	Low
ÇANKIRI	3	4	1	1	2	2	2	1	1	2	5	2	5	5	5	2,45	2,00	3,80	1,86	1,52	**1,73**	Low
ÇORUM	4	3	2	1	2	2	3	1	1	4	3	2	4	5	1	2,85	2,20	2,90	1,65	1,28	**1,50**	Low
DENİZLİ	5	5	5	2	3	5	5	3	2	5	5	5	4	3	5	4,50	3,95	4,40	3,96	3,48	**3,77**	High
DİYARBAKIR	5	4	4	1	2	5	5	1	1	4	3	2	3	4	2	4,00	2,80	2,60	2,08	1,46	**1,83**	Low
DÜZCE	2	2	3	1	3	1	2	1	2	5	5	3	2	5	4	2,05	2,45	3,15	1,29	1,54	**1,39**	Low
EDİRNE	4	2	1	1	2	1	3	1	1	1	2	1	4	5	1	2,45	1,75	2,50	1,23	0,88	**1,09**	Low
ELAZIĞ	2	4	2	1	3	2	3	1	1	4	5	3	3	1	3	2,30	2,50	2,70	1,24	1,35	**1,29**	Low
ERZİNCAN	4	3	5	1	3	5	2	1	2	2	5	4	4	5	4	3,70	2,15	4,15	3,07	1,78	**2,56**	Moderate
ERZURUM	4	4	3	1	2	5	4	2	1	4	4	2	2	5	4	3,45	2,95	2,75	1,90	1,62	**1,79**	Low
ESKİŞEHİR	4	2	1	1	2	2	5	2	1	5	3	3	3	5	3	2,55	3,20	3,30	1,68	2,11	**1,85**	Low
GAZİANTEP	5	5	5	2	3	5	5	1	1	3	5	3	4	3	5	4,50	3,00	3,60	3,24	2,16	**2,81**	Moderate
GİRESUN	3	2	2	1	2	2	2	1	1	4	3	1	5	1	5	2,30	1,90	2,80	1,29	1,06	**1,20**	Low
GÜMÜŞHANE	3	3	2	1	3	1	2	1	1	5	4	2	4	5	1	2,45	2,15	2,90	1,42	1,25	**1,35**	Low

BRANCH NAME	CREDIT RISKS						OPERATIONAL RISKS					CONTROL RISKS				RISK LEVELS			RESIDUAL RISK		RESIDUAL RISK	
	40%	15%	15%	10%	10%	10%	30%	30%	15%	10 %	15%	40 %	30 %	15 %	15%							
	Total Credit Portfolio Size (million TRY)	Close Monitoring Loan Ratio	Non-Performing Loan Ratio	Number of Investigations Related to Credit Transactions	Risk Point of Board of Auditors	Bad Cheque Ratios	Annual Average Cash Transaction Volume per Operatiom Personnel (Milyon TL)	Annual EFT (Electronic Fund Transfer) and Transfer Transaction Volume per Operration Personnel	Number of Investigations Related to Operational Transactions	Number of Expired Discrepancies	Internal Control Department Risk Point	Surveillance of Management	Efficiency and Adequacy of Personnel	Date of Last Audit	Ratio of Actions Taken Against Audit Findings	CREDIT RISK LEVEL	OPERATIONAL RISK LEVEL	CONTROL RISK LEVEL	RESIDUAL CREDIT RISK	RESIDUAL OPERATIONAL RISK	RESIDUAL RISK	
HAKKARİ	4	2	4	1	2	1	5	3	2	5	5	3	1	5	5	2,90	3,95	3,00	1,74	2,37	**1,99**	Low
HATAY	4	3	1	1	2	4	4	2	1	5	3	2	3	5	2	2,90	2,90	2,75	1,60	1,60	**1,60**	Low
ISPARTA	4	3	2	2	3	5	5	2	1	5	5	4	4	1	4	3,35	3,50	3,55	2,38	2,49	**2,42**	Moderate
MERSİN	2	5	1	1	3	4	3	1	1	2	4	3	4	4	4	2,50	2,15	3,60	1,80	1,55	**1,70**	Low
IĞDIR	3	4	1	1	2	2	3	1	2	3	3	3	4	5	2	2,45	2,25	3,45	1,69	1,55	**1,64**	Low
İSTANBUL	5	4	2	1	2	5	5	3	1	5	4	1	1	3	4	3,70	3,65	1,75	1,30	1,28	**1,29**	Low
İSTANBUL EMİNÖNÜ	5	4	3	1	2	5	5	2	1	5	5	3	5	5	5	3,85	3,50	4,20	3,23	2,94	**3,12**	Moderate
İSTANBUL GÜNEŞLİ	5	5	3	2	3	5	5	2	1	5	4	2	2	5	2	4,20	3,35	2,45	2,06	1,64	**1,89**	Low
İSTANBUL KADIKÖY	5	4	5	1	2	5	5	2	1	5	5	2	1	4	3	4,15	3,50	2,15	1,78	1,51	**1,67**	Low
İSTANBUL KARAKÖY	5	5	2	1	2	5	5	3	1	5	4	2	1	2	5	3,85	3,65	2,15	1,66	1,57	**1,62**	Low
İSTANBUL KOZYATAĞI	5	5	5	2	3	5	5	4	1	5	5	5	5	3	5	4,50	4,10	4,70	4,23	3,85	**4,08**	High
İSTANBUL MECİDİYEKÖY	5	5	5	1	2	5	5	2	1	5	4	2	2	5	2	4,30	3,35	2,45	2,11	1,64	**1,92**	Low
İSTANBUL OSMANBEY	5	5	2	1	3	5	5	3	2	4	3	1	1	5	4	3,95	3,55	2,05	1,62	1,46	**1,55**	Low
İSTANBUL TAKSİM	5	3	2	1	2	2	5	2	1	5	4	2	4	1	3	3,25	3,35	2,60	1,69	1,74	**1,71**	Low
İSTANBUL ÜSKÜDAR	5	5	5	2	3	5	5	3	1	5	4	3	4	5	4	4,50	3,65	3,75	3,38	2,74	**3,12**	Moderate
İSTANBUL ZEYTİNBURNU	5	5	2	1	2	5	5	2	2	5	5	2	2	5	3	3,85	3,65	2,60	2,00	1,90	**1,96**	Low
İZMİR	5	3	3	1	2	3	5	1	1	5	5	2	1	1	5	3,50	3,20	2,00	1,40	1,28	**1,35**	Low

BRANCH NAME	CREDIT RISKS						OPERATIONAL RISKS					CONTROL RISKS				RISK LEVELS			RESIDUAL RISK		RESIDUAL RISK	
	40%	15%	15%	10%	10%	10%	30%	30%	15%	10 %	15%	40 %	30 %	15 %	15%							
	Total Credit Portfolio Size (million TRY)	Close Monitoring Loan Ratio	Non-Performing Loan Ratio	Number of Investigations Related to Credit Transactions	Risk Point of Board of Auditors	Bad Cheque Ratios	Annual Average Cash Transaction Volume per Operatiom Personnel (Milyon TL)	Annual EFT (Electronic Fund Transfer) and Transfer Transaction Volume per Operration Personnel	Number of Investigations Related to Operational Transactions	Number of Expired Discrepancies	Internal Control Department Risk Point	Surveillance of Management	Efficiency and Adequacy of Personnel	Date of Last Audit	Ratio of Actions Taken Against Audit Findings	CREDIT RISK LEVEL	OPERATIONAL RISK LEVEL	CONTROL RISK LEVEL	RESIDUAL CREDIT RISK	RESIDUAL OPERATIONAL RISK	RESIDUAL RISK	
İZMİR BORNOVA	4	4	2	1	2	4	4	1	1	2	4	2	3	5	5	3,20	2,45	3,20	2,05	1,57	**1,86**	Low
İZMİR KARABAĞLAR	4	2	2	1	3	2	4	2	1	3	4	2	3	1	4	2,80	2,85	2,45	1,37	1,40	**1,38**	Low
İZMİR KARŞIYAKA	5	5	2	1	3	5	5	1	1	2	5	3	5	5	3	3,95	2,90	3,90	3,08	2,26	**2,75**	Moderate
İZMİR MENEMEN	4	2	1	2	2	4	4	2	1	5	4	2	4	5	4	2,85	3,05	3,35	1,91	2,04	**1,96**	Low
KARABÜK	2	2	1	1	2	1	2	1	1	2	3	2	4	5	4	1,65	1,70	3,35	1,11	1,14	**1,12**	Low
KARAMAN	3	3	1	1	2	4	2	1	1	2	4	1	3	3	1	2,50	1,85	1,90	0,95	0,70	**0,85**	Low
KARS	2	2	1	1	2	1	3	1	1	2	4	2	1	4	3	1,65	2,15	2,15	0,71	0,92	**0,80**	Low
KASTAMONU	3	5	1	1	3	3	4	1	1	3	5	2	4	5	4	2,80	2,70	3,35	1,88	1,81	**1,85**	Low
KAYSERİ	5	5	4	2	3	5	5	3	1	5	5	3	4	3	3	4,35	3,80	3,30	2,87	2,51	**2,73**	Moderate
KIRIKKALE	3	1	2	1	2	2	2	1	1	4	3	2	2	5	4	2,15	1,90	2,75	1,18	1,05	**1,13**	Low
KIRKLARELİ	2	2	1	1	2	1	2	1	1	2	3	2	2	5	4	1,65	1,70	2,75	0,91	0,94	**0,92**	Low
KIRŞEHİR	2	4	1	1	2	1	2	1	2	2	4	3	3	1	5	1,95	2,00	3,00	1,17	1,20	**1,18**	Low
KİLİS	4	4	5	2	3	5	4	2	1	5	4	3	4	5	4	3,95	3,05	3,75	2,96	2,29	**2,69**	Moderate
KOCAELİ	4	3	1	1	2	1	3	1	1	2	4	2	4	4	5	2,60	2,15	3,35	1,74	1,44	**1,62**	Low
KONYA	4	5	1	1	3	5	4	2	1	5	5	3	1	2	3	3,40	3,20	2,25	1,53	1,44	**1,49**	Low
KÜTAHYA	2	5	1	1	3	5	3	1	1	3	4	3	4	5	3	2,60	2,25	3,60	1,87	1,62	**1,77**	Low
MALATYA	4	4	3	2	3	5	4	2	1	5	5	3	4	5	5	3,65	3,20	3,90	2,85	2,50	**2,71**	Moderate
MANİSA	4	1	1	1	1	2	4	2	1	1	2	1	3	5	3	2,30	2,35	2,50	1,15	1,18	**1,16**	Low
KAHRAMANMARAŞ	4	5	1	1	3	5	4	3	1	5	5	3	5	3	5	3,40	3,50	3,90	2,65	2,73	**2,68**	Moderate
MARDİN	4	4	1	1	2	2	3	1	2	5	5	2	1	4	1	2,85	2,75	1,85	1,05	1,02	**1,04**	Low
MUĞLA	4	3	2	1	3	5	3	1	1	5	5	3	3	5	3	3,25	2,60	3,30	2,15	1,72	**1,97**	Low
MUŞ	2	3	1	1	3	4	2	1	1	2	4	3	3	1	4	2,20	1,85	2,85	1,25	1,05	**1,17**	Low
NEVŞEHİR	3	3	1	1	3	1	4	1	1	5	5	2	4	5	5	2,30	2,90	3,50	1,61	2,03	**1,78**	Low
NİĞDE	2	3	1	1	2	5	2	1	1	2	4	2	3	1	4	2,20	1,85	2,45	1,08	0,91	**1,01**	Low

BRANCH NAME	CREDIT RISKS						OPERATIONAL RISKS					CONTROL RISKS				RISK LEVELS			RESIDUAL RISK		RESIDUAL RISK	
	40%	15%	15%	10%	10%	10%	30%	30%	15%	10 %	15%	40 %	30 %	15 %	15%							
	Total Credit Portfolio Size (million TRY)	Close Monitoring Loan Ratio	Non-Performing Loan Ratio	Number of Investigations Related to Credit Transactions	Risk Point of Board of Auditors	Bad Cheque Ratios	Annual Average Cash Transaction Volume per Operatiom Personnel (Milyon TL)	Annual EFT (Electronic Fund Transfer) and Transfer Transaction Volume per Operration Personnel	Number of Investigations Related to Operational Transactions	Number of Expired Discrepancies	Internal Control Department Risk Point	Surveillance of Management	Efficiency and Adequacy of Personnel	Date of Last Audit	Ratio of Actions Taken Against Audit Findings	CREDIT RISK LEVEL	OPERATIONAL RISK LEVEL	CONTROL RISK LEVEL	RESIDUAL CREDIT RISK	RESIDUAL OPERATIONAL RISK	RESIDUAL RISK	
ORDU	4	5	1	1	3	3	5	3	1	5	3	2	2	4	5	3,20	3,50	2,75	1,76	1,93	**1,83**	Low
OSMANİYE	3	3	1	2	2	5	4	1	1	2	4	2	2	5	2	2,70	2,45	2,45	1,32	1,20	**1,27**	Low
RİZE	5	5	5	1	3	5	5	2	2	5	5	4	3	2	4	4,40	3,65	3,40	2,99	2,48	**2,79**	Moderate
SAKARYA	3	3	1	1	2	1	4	1	1	3	5	3	1	4	2	2,20	2,70	2,40	1,06	1,30	**1,15**	Low
SAMSUN	5	5	3	2	3	5	5	4	2	5	5	4	5	3	5	4,20	4,25	4,30	3,61	3,66	**3,63**	High
SİİRT	4	3	1	1	2	1	3	1	1	3	4	1	3	5	3	2,60	2,25	2,50	1,30	1,13	**1,23**	Low
SİNOP	3	3	1	1	3	3	4	2	1	5	3	2	3	5	3	2,50	2,90	2,90	1,45	1,68	**1,54**	Low
SİVAS	4	5	4	1	2	5	5	3	1	2	4	2	2	2	3	3,75	3,35	2,15	1,61	1,44	**1,54**	Low
TEKİRDAĞ	2	3	1	1	2	1	2	1	1	5	3	2	4	5	2	1,80	2,00	3,05	1,10	1,22	**1,15**	Low
TOKAT	3	5	1	1	2	5	3	1	1	5	5	2	3	4	4	2,90	2,60	2,90	1,68	1,51	**1,61**	Low
TRABZON	4	5	1	1	3	1	5	4	1	5	5	2	2	1	1	3,00	4,10	1,70	1,02	1,39	**1,17**	Low
TUNCELİ	3	3	1	1	3	4	3	1	1	4	4	2	4	5	3	2,60	2,35	3,20	1,66	1,50	**1,60**	Low
ŞANLIURFA	4	4	1	1	3	2	4	2	2	5	5	3	5	4	4	2,95	3,35	3,90	2,30	2,61	**2,43**	Moderate
ŞIRNAK	3	2	1	1	2	2	4	1	1	2	4	2	4	1	4	2,15	2,45	2,75	1,18	1,35	**1,25**	Low
UŞAK	4	2	1	1	2	1	5	3	1	5	5	3	2	5	2	2,45	3,80	2,85	1,40	2,17	**1,70**	Low
VAN	4	1	2	2	3	5	5	2	1	5	5	3	4	5	4	3,05	3,50	3,75	2,29	2,63	**2,42**	Moderate
YALOVA	3	4	1	1	3	1	4	2	1	5	3	1	3	2	5	2,45	2,90	2,35	1,15	1,36	**1,24**	Low
YOZGAT	2	1	1	1	2	2	3	2	1	5	4	3	4	5	3	1,60	2,75	3,60	1,15	1,98	**1,48**	Low
ZONGULDAK	4	2	1	1	3	1	5	1	1	5	5	2	3	5	3	2,55	3,20	2,90	1,48	1,86	**1,63**	Low

Appendix-3

ANNUAL AUDIT PLAN		
BRANCH NAME	**RESIDUAL RISK**	**RISK LEVEL**
ADANA	2.02	Moderate
AFYONKARAHİSAR	1.98	Low
AMASYA	2.57	Moderate
ANKARA	3.50	High
ANKARA ULUS	3.24	Moderate
ARTVİN	1.75	Low
BİNGÖL	0.98	Low
BURSA	2.73	Moderate
DENİZLİ	3.77	High
DÜZCE	1.93	Low
EDİRNE	1.51	Low
ERZİNCAN	2.42	Moderate
ERZURUM	2.00	Low
GÜMÜŞHANE	1.80	Low
HATAY	1.43	Low
İSTANBUL KOZYATAĞI	4.08	High
İSTANBUL OSMANBEY	1.21	Low
İSTANBUL ÜSKÜDAR	2.81	Moderate
İZMİR KARŞIYAKA	2.24	Moderate
İZMİR MENEMEN	1.35	Low
KASTAMONU	1.76	Low
KİLİS	2.88	Moderate
MALATYA	2.56	Moderate

ANNUAL AUDIT PLAN		
BRANCH NAME	**RESIDUAL RISK**	**RISK LEVEL**
MANİSA	1.13	Low
MUĞLA	1.31	Low
OSMANİYE	1.29	Low
SAMSUN	3.63	High
UŞAK	1.80	Low
VAN	3.12	Moderate
YOZGAT	1.10	Low