



TC

MINISTRY OF FINANCE

GENERAL DIRECTORATE OF BUDGET AND FINANCIAL CONTROL



Public Internal Control Guide

Control environment

Risk management

Control activities

Information and communication

Monitoring

This guide has been prepared within the framework of the TR07-IBFI-02 Twinning Project, funded by the European Union.



VERSION 1.0

CONTENTS

LIST OF ABBREVIATIONS.....	VI
----------------------------	----

INTRODUCTION	1
Control	1
Users of the Guide.....	5
Responsibilities in Internal Control.....	6

CHAPTER ONE

CONTROL ENVIRONMENT

1. INTRODUCTION	7
2. CONTROL ENVIRONMENT STANDARDS	8
VALUES AND INTEGRITY.....	11
2.1.1. The Concept of Ethics.....	11
2.1.2. Ethics Training	13
2.2. MISSION, ORGANIZATIONAL STRUCTURE AND DUTIES	14
2.2.1. Mission.....	14
2.2.2. Organizational Structure and Tasks.....	14
2.2.3. Job Descriptions.....	15
2.2.4. Sensitive Tasks	17
2.2.5 Monitoring Task Results	17
2.3. PERSONNEL COMPETENCE AND PERFORMANCE.....	18
2.3.1. Human Resources Management.....	18
2.3.2. Basic Elements of Human Resources Management	19
2.4. DELEGATION OF AUTHORITY.....	20
2.4.1. Delegation of Authority and Workflow Processes.....	20
2.4.2. Delegation of Authority and Responsibility.....	20
2.4.3. Considerations to be Taken into Account in Delegation of Authority	20
2.4.4. Delegation of Signature Authority.....	21

PART TWO

RISK MANAGEMENT

1. INTRODUCTION	22
2. RISK ASSESSMENT STANDARDS.....	22
3. BENEFITS THAT RISK MANAGEMENT CAN PROVIDE TO THE ADMINISTRATION.....	24
4. CRITICAL SUCCESS FACTORS FOR EFFECTIVE RISK MANAGEMENT	24
5. RISK MANAGEMENT STRATEGY	24
6. DUTIES, POWERS AND RESPONSIBILITIES.....	26

6.1. Senior Management	27
6.2. Internal Control Monitoring and Steering Committee (ICMC)	27
6.3. Administrative Risk Coordinator (ARC)	28
6.4. Unit Risk Coordinator (UCC)	28
6.5. Sub-Unit Risk Coordinator (SUCC)	28
6.6. Employees	29
6.7. Internal Audit Unit	29
6.8. Strategy Development Units	29
6.9. MYK Central Harmonization Unit (MYK CHU)	29
7. RISK MANAGEMENT PROCESS.....	29
7.1. Identifying Risks.....	31
7.2. Assessing Risks.....	34
7.3. Responding to Risks.....	39
7.4. Reviewing and Reporting Risks.....	44
7.4.1. Risk Review.....	44
7.4.2. Reporting	45
8. LEARNING FROM EXPERIENCES.....	45
RISK MANAGEMENT APPENDICES	47
RY Appendix 1: Method to be Followed in Identifying, Assessing and Recording Risks	47
RY APPENDIX 2: Risk Rating Form.....	49
RY APPENDIX 3: Risk Record Form	51
RY APPENDIX 4: Consolidated Risk Report.....	53
RY APPENDIX 5: Sample Risk Assessment Criteria Table	55
RY APPENDIX 6: Case Study on Natural and Residual Risk.....	57

CHAPTER THREE

CONTROL ACTIVITIES

1. INTRODUCTION	58
2. CONTROL ACTIVITY STANDARDS	58
3. CONTROL ACTIVITIES PLANNING PROCESS.....	59
4. CLASSIFICATION OF CONTROL ACTIVITIES.....	60
4.1. Directive Controls	60
4.2. Preventive Controls.....	61
4.3. Detection Controls.....	61
4.4. Corrective Controls	61
5. CONTROL ACTIVITY METHODS	61
5.1. Decision Making and Approval	62
5.2. Separation of Duties.....	62
5.3. Double Signature Method.....	63
5.4. Data Reconciliation.....	63

5.5. Monitoring Procedures	63	5.6. Preliminary Financial Control	64
5.7. Procedures Related to Accounting Transactions	64		
5.8. Anti-Corruption Procedures	64		
5.9. Access to Assets and Information.....	64	5.10. Documentation, Archiving, and Storage of Information.....	64
5.11. Business Continuity Plans.....	65	5.12. Information Technology Control Activities	65
5.13. Evaluation of the Benefits and Costs of Control Activities	66		
6. IMPLEMENTATION STAGES OF CONTROL ACTIVITIES.....	66		
7. STEPS TO BE FOLLOWED WHEN DETERMINING AND IMPLEMENTING CONTROL ACTIVITIES	67		
CONTROL ACTIVITIES APPENDIX	68		
KF Appendix 1: Sample Control Activity List.....	68	KF Appendix 2: Benefit-Cost Analysis Examples	74

CHAPTER FOUR

INFORMATION AND COMMUNICATION

1. INTRODUCTION	75
2. INFORMATION AND COMMUNICATION STANDARDS.....	75
3. ROLES AND RESPONSIBILITIES IN INFORMATION AND COMMUNICATION	76
3.1. Senior Manager	76
3.2. Internal Audit Unit	76
3.3. Spending Authority	76
3.4. Implementation Officer	77
3.5. Accounting Officer.....	77
3.6. Strategy Development Units	77
3.7. Financial Management and Control Center Harmonization Unit (MYK MUB)	77
4. INFORMATION	78
4.1. Characteristics of Information.....	78
4.2. Information Management	78
4.2.1. Planning Information Needs.....	79
4.2.2. Creating and Collecting Information.....	80
4.2.3. Organizing Information.....	80
4.2.3.1. Recording, Filing, and Archiving Information.....	81
4.2.4. Using and Sharing Information.....	82
4.2.5. Reviewing and Protecting Information.....	83
4.2.5.1. Information Security.....	84
4.2.5.1.1. Information Security Management System.....	84
5. MANAGEMENT INFORMATION SYSTEMS (MIS).....	85
5.1. MIS Installation Stages	85

5.1.1. Establishment of the MIS Working Team	85
5.1.2. Planning and Execution of MIS Setup Activities	85
5.1.3. Monitoring and Evaluation of the MIS Setup Process.....	86
6. COMMUNICATION.....	86
6.1. Internal and External Communication	87
7. REPORTING	89
8. REPORTING IRREGULARITIES AND CORRUPTION	90
8.1. Concepts of Irregularity, Corruption, and Informing	90
8.2. Scope of Notifications.....	90
8.2.1. Reports and complaints regarding violations of ethical values	91
8.2.2. Complaints regarding irregularities and corruption.....	91
8.2.3. Complaints by Public Officials.....	91
8.3. Responsibility in Detecting Errors, Irregularities, and Corruption	91
8.4. Informing System.....	91
9. INTER-UNIT RELATIONS.....	93
9.1. Communication Between MYK MUB and SGBs.....	93
9.2. Communication Between SGBs and Spending Units	94
INFORMATION AND COMMUNICATION SECTION APPENDICES	95
BI APPENDIX 1: Legislation in the Field of Information and Communication.....	95
BI APPENDIX 2: Commonly Used Communication Methods	96

CHAPTER FIVE

MONITORING

1. INTRODUCTION	98
2. MONITORING STANDARDS	98
3. ROLES AND RESPONSIBILITIES	99
3.1. Monitoring Roles and Responsibilities in Public Administrations.....	99
3.1.1. Senior Manager.....	99
3.1.2. Internal Audit Unit	99
3.1.3. Internal Control Monitoring and Steering Committee (ICMS).....	99
3.1.4. Strategy Development Unit (SDU).....	99
3.1.5. Spending Authorities	100
3.1.6. Other Managers and Employees	100
3.2. Other Roles and Responsibilities Related to Monitoring.....	100
3.2.1. MYK MUB.....	100
3.2.2. External Audit.....	101
4. MONITORING METHODS	101
4.1. Continuous monitoring	101
4.2. Special Considerations	101

4.2.1. Evaluation Process	102	4.2.2.	
Reporting of Evaluation Results	103	4.2.3. Monitoring of Evaluation	
Reports	104		
5. ACTIONS TO BE TAKEN BY THE MINISTRY OF HEALTH REGULATIONS REGARDING INTERNAL AUDIT REPORTS	104		
MONITORING SECTION APPENDICES	105		
APPENDIX 1. Sample Internal Control System Questionnaire.....			
105 APPENDIX 2. Internal Control System Evaluation Report	121		
CONTRIBUTORS TO THE PREPARATION OF THE PUBLIC INTERNAL CONTROL GUIDE.....	123		

LIST OF ABBREVIATIONS

ARC	: Sub-Unit Risk Coordinator
BI	Information and Communication
B�MER	Prime Minister's Communication Center
BRK	Unit Risk Coordinator
BT	Information Technologies
COSO	Committee of Sponsoring the Treadway Commission Organizations of the Treadway Commission)
SWOT	Strengths and Weaknesses, Opportunities and Threats
INTOSAI	International Organisations of Supreme Audit Institutions (IOSI) Institutions)
IDKK	Internal Audit Coordination Board
HR	Human Resources Management
TWO	Internal Control Monitoring and Steering Committee
RACE	Administrative Risk Coordinator
TRACE	: Monitoring
KO	: Control Environment
KF	Control Activities
KRY	Corporate Risk Management
MERNIS	Central Population Administration System
MUB	Central Coordination Unit
MYK	Financial Management and Control
MYK MUB	Financial Management and Control Center Harmonization Unit
PESTLE	: Political, Economic, Social, Technological, Legal and Environmental Social, Technological, Legal and Environmental)
RSB	Risk Strategy Document
RY	Risk Management
SGB	Strategy Development Unit
TSE	Turkish Standards Institute
YBS	Management Information System
Turkish Grand National Assembly	Turkish Grand National Assembly
UYAP	National Judicial Network Information System

ENTRANCE

Since the late twentieth century, governments worldwide have focused on implementing mechanisms to improve performance. 'Good governance,' a concept introduced to serve this purpose, has recently become a guiding principle for both the public and private sectors.

Within the framework of good governance principles, ensuring accountability, enhancing transparency, providing administrative flexibility through delegation of authority and responsibility, and meeting citizen expectations through a results-oriented management and budgeting approach have been prominent elements aimed at providing higher quality public services.

The improvement in the quality of public services has brought about a need for a goal-oriented approach and the effective, economical, and efficient use of public resources. This has necessitated the use of effective tools in many areas related to financial management and control processes, from the organizational structure of public institutions to communication and monitoring. The most important management tool adopted in this reform process is *the internal control system*.

Internal Control

Internationally recognized **internal control** provides reasonable assurance that an organization will achieve its objectives. Internal control is a system designed to ensure compliance with regulations, reliability of financial and managerial reporting, effectiveness and efficiency of operations, and protection of assets. The best-known model of this system, *the Committee of Sponsoring Organizations (COSO)* framework, aims to ensure that the organization's operations and activities comply with regulations, that financial and managerial reporting is reliable, and that operations are effective and efficient, thus protecting assets.

The internal control system developed by COSO, consisting of *control environment, risk management, control activities, information and communication, and monitoring* components, is a model accepted as a reference by the International Organization of Supreme Audit Institutions (INTOSAI), the European Commission, and similar international organizations. Figure 1 shows the components of internal control.

Figure 1: COSO Cube



Our country, which is currently conducting membership negotiations with the European Union, has been undergoing a reform process since the early 2000s to strengthen its public internal control system.

In this process, the main elements of the internal control model recommended by the European Commission to all candidate countries and compatible with COSO can be summarized as follows : **a financial management and control (FMCC) system based on managerial responsibility and accountability**, functionally independent **internal audit activity** , and a **Central Harmonization Unit (CHU)** responsible for harmonizing these two areas across the entire public sector .

In its broadest sense , **MYK** refers to the processes of managing and controlling public resources. Accordingly, public administrators at all levels are responsible for establishing and maintaining an effective MYK (Management, Evaluation, and Control) system to fulfill their duties regarding planning, programming, budgeting, budget implementation, accounting, control, reporting, archiving, and monitoring of the resources under their management. is responsible.

Internal auditing helps managers in fulfilling this responsibility and achieving goals. Its function is to provide objective assurance and consultancy services regarding the compliance of the existing MYK system with established methods and standards and sound financial management principles, based on risk management.

Furthermore, a **central harmonization activity** is deemed necessary to establish and develop methodologies, legislation, and standards based on internationally accepted standards and best practices in the field of vocational training and internal auditing in the public sector, to coordinate and monitor their implementation, and to provide the necessary training .

Mevzuat : 5018/55

İç Kontrolün Tanımı

İdarenin Amaçları ve Politikaları

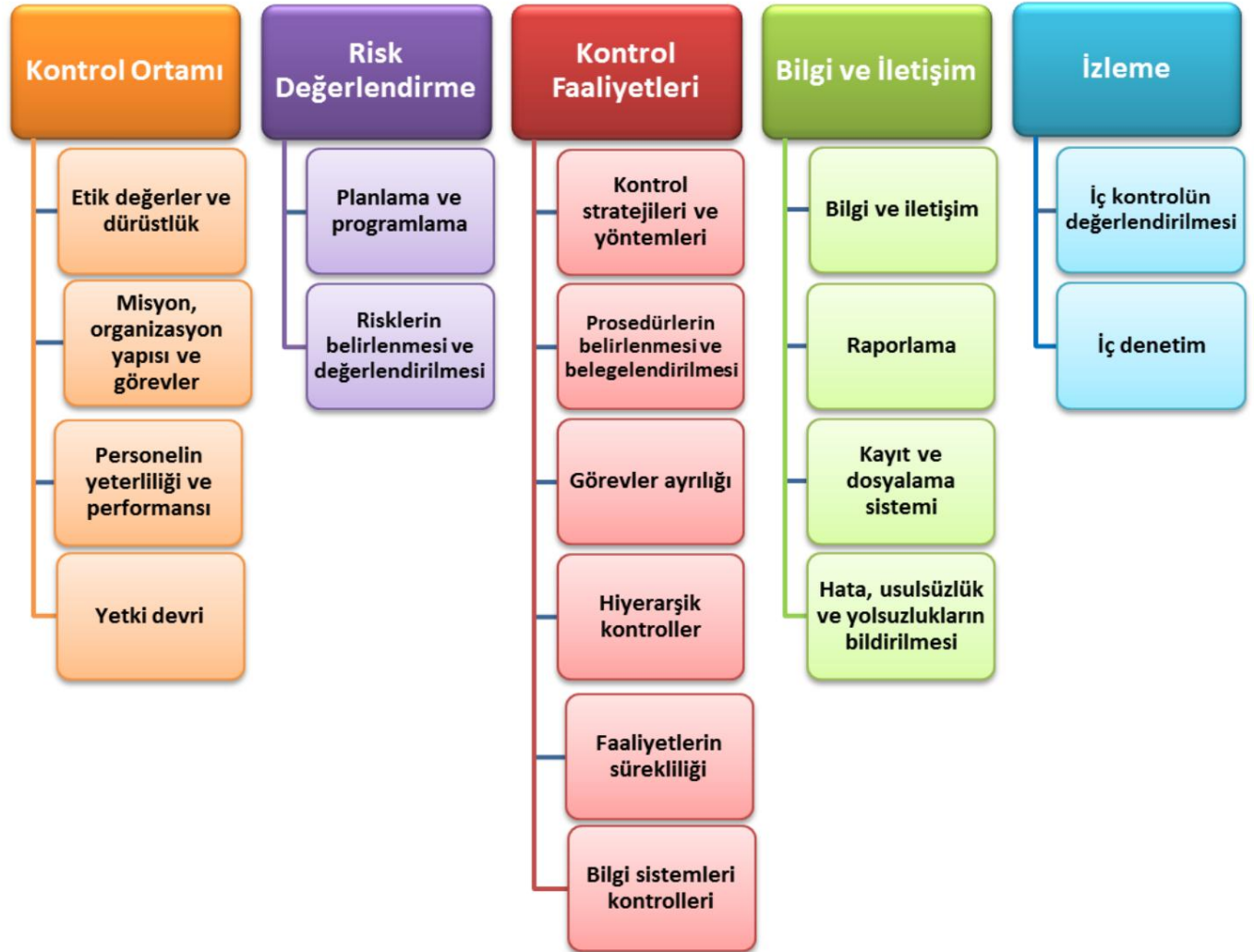


In light of these developments, our country aims to increase transparency and accountability in public financial management. It has taken significant steps towards strengthening and establishing an effective internal control system.

The most important of these steps, the *Public Financial Management and Control Law No. 5018*, adopted in 2003, defined the functioning of the internal control system and the roles and responsibilities of the actors in the system. It assigned the Ministry of Finance the task of determining standards and methods for internal control processes and providing guidance to public administrations by ensuring coordination in this area. In line with this task, the Ministry of Finance published the *Public Internal Control Standards Circular* in the Official Gazette dated December 26, 2007, and numbered 26738 .

Figure 2: Internal Control Components and Standards

İÇ KONTROL BİLEŞENLERİ VE STANDARTLARI



In this context, the fundamental principles regarding the establishment and implementation of the public internal control system in our country... Documents and regulations are located in Box 1.

Box 1: Framework for the Internal Control System



This Guide, prepared based on all these documents and regulations, aims to support decision-making and implementation processes for better governance and thus contribute to the rational use of public resources. The Guide, whose preparation began in early 2010 and was completed in the last quarter of 2011, is the result of the dedicated work of experts from the United Kingdom and our country within the framework of a twinning project funded by the European Union.

The guide was discussed in workshops held with the participation of Strategy Development Unit (SDU) managers of public administrations and revised by working groups established at the Ministry of Finance. The resulting draft guide has been published on the website for comments and suggestions. It was sent to the relevant public administrations. The Guide was finalized based on the opinions and evaluations received from the public administrations.

The guide is designed as a roadmap to shed light on the application of internal control standards, explaining the fundamental elements of internal control with methods, tools, and examples that all stakeholders can use.

While this Guide is prepared in a way that allows for revisions over time to reflect changing conditions and needs, administrations may also use different tools according to their requirements; however, these tools must not contradict the fundamental requirements set forth in the Guide.

This Guide is composed of **5 main sections** based on Public Internal Control Standards . Following the introduction, there is a table showing the roles and responsibilities of the key actors in the financial management and control system.

The first section addresses the building blocks of the control environment , including ethical values and integrity, mission, organizational structure and responsibilities, personnel competence and performance, and delegation of authority. Conceptual explanations, legislation, and implementation tools are included.
The second section discusses the importance and objectives of risk management , the stages of the risk management process and the roles and responsibilities of the actors involved, and the communication and reporting tools that can be used with the Risk Strategy Document (RSB).
The third section examines a range of control activities closely related to risk management , including control strategies and methods, the establishment and documentation of procedures, the principle of separation of duties, hierarchical controls, continuity of operations, and information processing controls. These activities include approval, authorization, verification, account reconciliation, etc.
In the fourth chapter, within the framework of the information and communication component, the concept and management of information, the functioning of Management Information Systems (MIS), internal and external communication tools, and reporting mechanisms are evaluated.

Chapter five describes the roles and responsibilities of the Financial Management and Control Center Harmonization Unit (FMCU) for the public sector as a whole, and the SGBs for each public administration, as well as the monitoring methods and tools, within the scope of regularly *monitoring* and evaluating the internal control system.

Guide Users

The guide will contribute to the decisions and activities of the managers and personnel, especially those listed below. It is intended to provide this.

- **Senior executives** responsible for establishing, overseeing, and monitoring an adequate and effective MYK (Centralized Management System)
- **Spending authorities** who, within their areas of responsibility and authority, are responsible for ensuring the functioning of internal control regarding administrative and financial decisions and transactions.
- The Ministry of Finance, which carries out the central coordination task in the MYK field, **relevant managers and employees**
- Development of internal control systems and implementation of standards in public administrations
SGB managers and personnel conducting studies on this matter
- **Implementing parties** involved in the financial transaction process and accountable to spending authorities.
officials
- **Others** who are responsible for activities carried out in the MYK field within their units
managers
- **All employees** working in public administrations
- **Internal personnel** responsible for evaluating the effectiveness of the MYK system and reporting to senior management.
audit units
- **External auditors** responsible for examining the accounts, financial transactions and activities of public administrations, as well as their internal control systems, and reporting to the Turkish Grand National Assembly on the effective, economical, efficient and lawful use of resources .

Figure 3: Internal Control Legislation



Roles and Responsibilities in Internal Control

Senior management: It is the responsibility of the senior management to ensure the establishment of an adequate and effective internal control system within the administration, to monitor its operation, and to improve it by taking necessary measures. The senior management owns the internal control system. While generally undertaking the monitoring task, the senior management is responsible for ensuring that the organization's activities are carried out in line with its objectives and for ensuring the proper functioning of the internal control system.

On the other hand, information about the compliance studies with the Public Internal Control Standards carried out in the public administrations included in the annexes (1) and (II/B) to the Law No. 5018 is given to the relevant Minister by the senior manager in January of each year.

Unit managers

(spending

authorities):

Effective in their units

an internal control system

It is responsible for creating, implementing and monitoring, and improving weaknesses.

Strategy Development

Unit Managers:

Internal control system in spending units

To provide coordination in And the creation, implementation and development of, and to provide training and guidance services. from providing is responsible.

Employee:

Internal control is part of the job for all personnel.

Everyone working within the organization plays a role in implementing the internal control system. Internal control is not a task to be carried out solely by personnel in one unit; it is a process embedded in the activities of everyone working within the organization. Therefore, it should not be considered an additional job or task.

Internal Audit Unit:

To continuously review the design and operation of the internal control system, to identify its strengths and weaknesses, and by providing assessments and recommendations for the improvement of the internal control system. It contributes to its development.



Financial Management and Control Center Harmonization Unit (Ministry of Finance):

It is responsible for establishing, developing, and harmonizing standards and methods for internal control processes, ensuring coordination, and providing guidance services to administrations.

Those outside the organization (service users, stakeholders, etc.):

Individuals outside the organization also play an important role in the internal control process. These individuals can provide useful information that can contribute to the achievement of the organization's objectives. However, these groups cannot be held responsible for the design, implementation, and proper functioning of the internal control system within the organization.



Court of Auditors:

According to the provisions of the Court of Accounts Law No. 6085, it evaluates the functioning of internal control systems in public administrations. As an external audit body, it assesses whether the internal control system of the public administration is functioning properly during its regularity audits. In this context, it examines internal control assurance statements signed by senior managers and spending authorities, and internal audit reports.

also takes into consideration.

CHAPTER ONE

CONTROL ENVIRONMENT

1. INTRODUCTION

According to the COSO Model, the control environment creates awareness of internal control among employees within an organization, thus laying the foundation for other components of internal control. The control environment is a fundamental component of the internal control system.

A robust control environment is essential for the proper functioning of internal control systems in public administrations. Problems in the control environment will negatively impact the functioning of other components.

A well-functioning control environment refers to a work environment where the organization's goals are known, duties and responsibilities are clearly defined, the organizational structure demonstrates reporting and hierarchical relationships, human resources practices are bound by objective rules, management and personnel embrace ethical values, personnel are provided with the necessary training and equipment to improve their competence, and managers set an example for employees by adhering to controls.

In this context, the control environment generally refers to the organizational culture, encompassing aspects such as the organization's internal control awareness, values, working methods and procedures, and the relationships between employees and managers. The fundamental elements of the control environment are summarized in KO Box 1.

KO Box 1: Basic Elements of the Control Environment:**Key Elements of the Control Environment**

- Principles of personal and professional integrity
- Adoption of ethical values by management and staff
- Supportive attitude of senior management towards internal control
- Corporate (organizational) structure
- Professional competence and performance of personnel
- Human resources policies and practices
- Management philosophy and way of doing business
- Delegation of Authority

Internal control is influenced by the historical and cultural structure of the organization. Every individual within the organization should embrace and practice personal and professional integrity and ethical values. To ensure this, managers should conduct performance evaluations that encourage ethical behavior through approaches that support internal control.

Management and employees should create and maintain a positive and supportive environment for the internal control system. Management's continuous monitoring of the internal control system, adherence to ethical guidelines, and setting an example for employees by complying with control activities demonstrate ownership of the internal control system. Evaluations conducted by managers should encourage the effective, economical, and efficient execution of activities in accordance with ethical guidelines. Performance evaluations should be conducted with these considerations in mind.

When the internal control system is embraced by top management, other employees' confidence in the system's functioning increases, and the foundations for a robust control environment are laid. If top management does not embrace the internal control system, employees will be reluctant, and the organization will not be able to achieve its goals. Therefore, managerial support for the internal control system is of paramount importance.

The establishment of an internal audit unit by a senior executive to conduct audits and provide consultancy on the design and operation of the internal control system is one of the most important indicators that they support and own the internal control system.

The organizational structure of the institution should clearly show the distribution of authority and responsibility. Sanctions and accountability should be defined in parallel with authority and responsibilities. The most fundamental tool that can be used to ensure accountability is reporting. Therefore, the organizational structure needs to demonstrate reporting and hierarchical relationships.

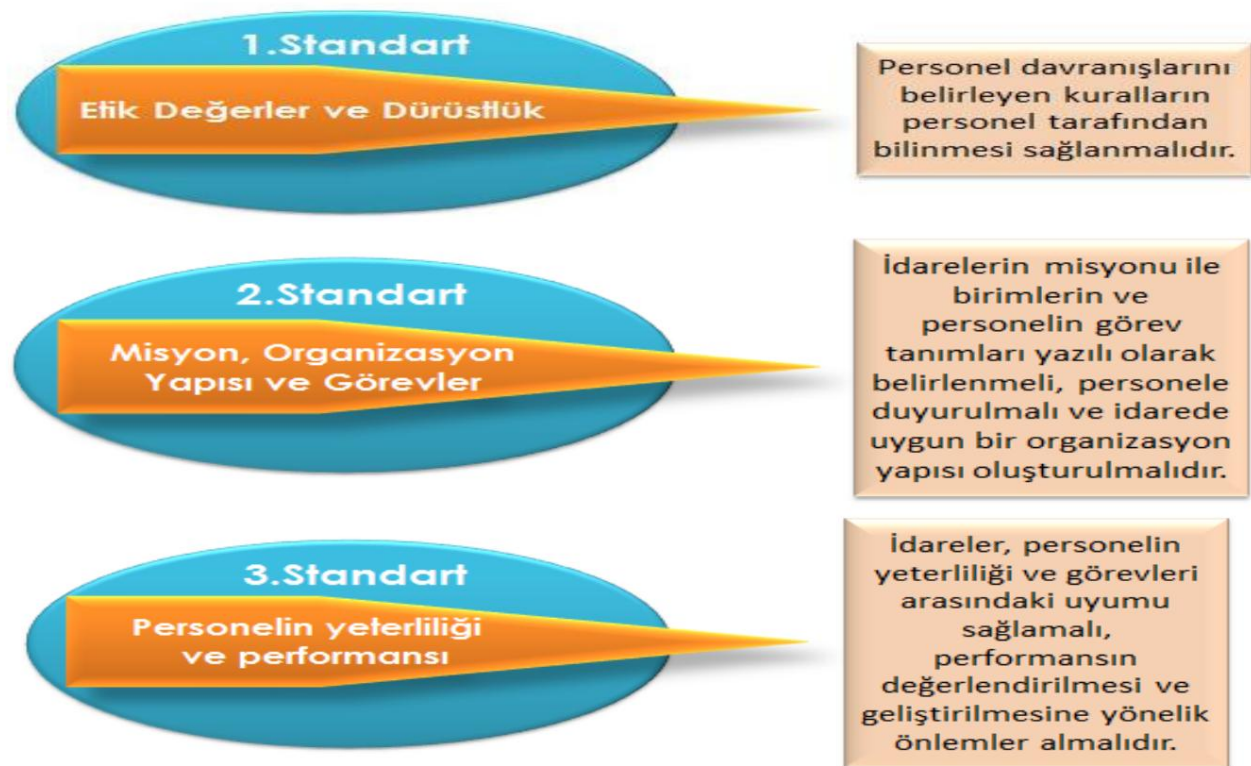
It is crucial for the quality of the control environment that employees know their duties and responsibilities and understand how their activities contribute to the organization's goals. Employees' adherence to personal and professional integrity and the adoption of ethical values are essential for the effective, economical, and efficient conduct of operations. Prioritizing the employment of skilled and expert individuals in human resources practices will help to increase awareness of control.

In a well-functioning control environment, the mission, organizational structure, and duties of public administration should be predetermined, and personnel performance should be evaluated at regular intervals.

2. CONTROL ENVIRONMENT STANDARDS

Four standards related to the control environment have been defined in the Public Internal Control Standards.

KO Box 2: Control Environment Standards:





Powers and authorities in administrations

The boundaries of its era must be clearly defined and in writing.

It must be reported. Transferred

Authority should be delegated taking into account the importance and risks of the delegation.

To better understand the Public Internal Control Standards and to guide their implementation. This section includes explanations regarding the relevant legislation and standards.

This text focuses on the methods necessary to ensure that ethical values and principles of integrity, which are of great importance for a well-functioning organization, are embraced by both senior management and personnel.

The document outlines the mission, organizational structure, and responsibilities, as well as criteria for evaluating staff competence and performance. It also clarifies how delegation of authority should occur, a key aspect of accountability.

Several examples of regulations relating to Control Environment elements are shown in KO Box 3:

KO Box 3. Main Legislation Regarding the Control Environment

KONTROL ORTAMI STANDARTLARI	İLGİLİ MEVZUAT
1. Etik Değerler ve Dürüstlük	• 5176 Sayılı Kamu Görevlileri Etik Kurulu Kurulması ve Bazı Kanunlarda Değişiklik Yapılması Hakkında Kanun • 2531 Sayılı Kamu Görevlerinden Ayrılanların Yapamayacakları İşler Hakkında Kanun • 3628 Sayılı Mal Bildiriminde Bulunulması, Rüşvet ve Yolsuzluklarla Mücadele Kanunu • Kamu Görevlileri Etik Davranış İlkeleri ile Başvuru Usul ve Esasları Hakkında Yönetmelik • Kamu Görevlileri Etik Rehberi • Konuya İlişkin Başbakanlık Genelgeleri • Kamu Görevlileri Etik Kurulu İlke Kararları
2. Misyon, Organizasyon Yapısı ve Görevler	• 3046 Sayılı Bakanlıkların Kuruluş ve Görev Esasları Hakkında Kanun • 217 Sayılı Devlet Personel Başkanlığı Kuruluş ve Görevleri Hakkında Kanun Hükmünde Kararname • İdarelerin teşkilat yapılarını düzenleyen mevzuat • Kamu İdareleri İçin Stratejik Planlama Kılavuzu

3.	Personelin Yeterliliği ve Performansı	• 657 Sayılı Devlet Memurları Kanunu / 2802 Sayılı Hakim ve Savcılar Kanunu / 2914 Sayılı Yüksek Öğretim Personel Kanunu / 926 Sayılı Türk Silahlı Kuvvetleri Personel Kanunu / 3269 Sayılı Uzman Erbaş Kanunu / 3466 Sayılı Uzman Jandarma Kanunu / 4678 Sayılı Türk Silahlı Kuvvetlerinde İstihdam Edilecek Sözleşmeli Subay ve Astsubaylar Hakkında Kanun • Kamu Görevlerine İlk Defa Atanacaklar İçin Yapılacak Sınavlar Hakkında Yönetmelik • Özürlülerin Devlet Memurluğuna Alınma Şartları İle Yapılacak Yarışma Sınavları Hakkında Yönetmelik • İdarelerin hazırladıkları özel yönetmelikler (uzman, kontrolör, müfettiş vb.) • Aday Memurların Yetiştirilmelerine İlişkin Genel Yönetmelik • Yetiştirilmek Amacıyla Yurt Dışına Gönderilecek Devlet Memurları Hakkında Yönetmelik • Kamu Kurum ve Kuruluşlarında Görevde Yükselme ve Unvan Değişikliği Esaslarına Dair Genel Yönetmelik • Yükseköğretim Üst Kuruluşları İle Yükseköğretim Kurumları Personeli Görevde Yükselme ve Unvan Değişikliği Yönetmeliği
4.	Yetki Devri	• 3046 Sayılı Bakanlıkların Kuruluş ve Görev Esasları Hakkında Kanun • 2547 Sayılı Yüksek Öğretim Kanunu • 5393 Sayılı Kanun • İdarelerin teşkilat yapılarını düzenleyen mevzuat • Harcama Yetkilileri Hakkında 1 Seri No'lu Genel Tebliğ

2.1. ETHICAL VALUES AND HONESTY

2.1.1. The Concept of Ethics

Ethics is the set of behaviors that should be followed or avoided in the performance of various professions. It is defined as such.

The concept of ethics in public administration applies to public officials. It refers to expected standards and principles of behavior.

Ethics is the totality of checks and balances that public officials use in their work to limit public power.

In public administration, ethics are important in preventing the misuse of public power or its use in ways that are contrary to the public interest.



The presence of ethical awareness in state administration, from top to bottom, guarantees the proper functioning of the system.

Unethical practices in public administration, first and foremost, diminish trust in the legal system and the state. As a result, rule-breaking becomes a widespread behavior across all segments of society.

In public administrations, ethical values should permeate all decision-making processes and activities at all levels.

With the establishment of an ethical framework, practices such as setting clear standards regarding unethical behavior, defining the boundaries of personal relationships in public administration, and declaring all of these will be implemented.

Furthermore, managers should set an example for their employees, fostering a corporate culture based on ethical values. It is of great importance in terms of settlement.

Law No. 5176 on the Establishment of the Public Officials Ethics Board and Amendments to Certain Laws defined the ethical conduct principles that public officials must adhere to, such as transparency, impartiality, honesty, accountability, and safeguarding the public interest, and the Public Officials Ethics Board was established to oversee their implementation.

The Regulation on Ethical Conduct Principles and Application Procedures for Public Officials includes the ethical conduct principles and the Ethical Agreement document that public officials are obliged to follow while performing their duties.

The ethical conduct principles that public officials must adhere to are shown in Figure 1.

KO Figure 1: Principles of Ethical Conduct



The Public Officials Ethics Guide, published by the Public Officials Ethics Board, details the ethical conduct rules expected of employees and managers in public administrations.

Key Ethical Behaviors Expected from Public Officials

• Always adhering to high ethical standards, acting in the public interest, and ensuring the public's trust in the state and... Efforts should be made to increase public trust in public officials.
• Adhering to written rules, ethical principles, and values when performing duties, using and obtaining public resources, and purchasing goods and services from external sources.
• Showing respect to colleagues and users, acting impartially and fairly.
• Taking into account the views of colleagues and service users in the decision-making process participation.
• Recognizing and publicizing the good work done by colleagues.
• Public office and resources should not be used for personal gain, and relatives, friends, and acquaintances should not be given preferential treatment in public services.
• Be mindful of potential and actual conflicts of interest.
• Taking responsibility for one's actions and decisions.
• Completing asset declaration forms on time, completely and accurately, and reporting assets Announcing any increase in case.
• Not working a second job outside of public service that is prohibited by law.
• Avoid entering into private business relationships with individuals or firms affiliated with the institution where you work.
• Warning other public employees whose behavior does not comply with ethical principles, and if no results are obtained, referring the matter to the relevant authorities.

In the public sector, managers perform their duties as follows:

• They must inform all employees about the organization's general aims, main objectives, and values.
• A positive work environment should be created where behavioral expectations are clearly defined and any violations are identified and corrected.
• They must accept full responsibility for the organization's activities.
• When selecting personnel for senior positions, they should consider their merit and current behavior and development potential
• They must treat all personnel fairly, equally, and impartially.
• They should resolve problems and disputes fairly and quickly.
• They must be consistent, reliable, predictable, fair, and objective in their decisions and actions.
• They should set a good example personally regarding ethical principles and values.
• Here are the highest possible standards to emulate in terms of productivity and effectiveness. They must continue.

2.1.2. Ethics Training

One of the essential prerequisites for establishing an organizational culture based on ethical principles and values is ethics training. Personnel at all levels employed in public institutions and organizations must be informed about ethical conduct principles and their responsibilities related to these principles.

According to the Public Officials Ethics Guide, managers of institutions and organizations are obligated to ensure that ethical conduct principles are included in the basic, preparatory, and in-service training programs applied to public officials.

2.2. MISSION, ORGANIZATIONAL STRUCTURE AND DUTIES

The second standard of the Control Environment involves establishing an appropriate organizational structure within the administration. It outlines the duties, authorities, and responsibilities of the unit and its personnel.

The administration's mission statement indicates its purpose and fundamental function within the state structure. The organizational structure ensures the control and oversight of the tasks performed to achieve the administration's aims and objectives. The administration's mission and organizational structure guide the tasks it undertakes. These complementary elements form an important foundation for the other components of the internal control system.

2.2.1. Mission

Public administrations define their mission, vision, aims, objectives, and strategies in their strategic plans. As stated in the Strategic Planning Guide for Public Administrations, the mission can be defined as the reason for an organization's existence. From this perspective, the mission encompasses all services and activities offered by the administration.



In other words, the mission statement is the answer to the questions of what public administration does, how it does it, and for whom it does it. For public administration to be guided by a sound, realistic, and participatory process, the mission statement should be defined and developed over time in line with evolving conditions and needs. It would be appropriate to include the views of personnel and stakeholders in the creation or updating of the mission statement.

Public administrations should consider the following points in their mission statements:

- The mission should be stated in current, precise, and clear terms.
- The mission should be related to the purpose of the administration, not the process of delivering the service.

- When defining the mission, the duties and powers granted to the administration by legal regulations are taken into consideration.
- The mission statement includes the individuals and organizations served by the public administration and the services offered by the organization.

KO Box 4: Example Mission Statement

"A Ministry of Finance that develops, implements, and monitors fiscal policy in a participatory manner with all stakeholders." (Ministry of Finance 2013-2017 Strategic Plan)

For public administrations, the mission is of paramount importance, and its successful implementation requires personnel to have sufficient knowledge of the administration's mission. Knowing and accepting the mission will guide management decisions and administrative activities, and help personnel understand their roles within the administration. To this end, it is necessary to first define the mission in writing, communicate it to all personnel, and develop a system for its adoption by relevant personnel. Furthermore, it is essential that the job descriptions of the administration's sub-units are defined in writing in accordance with the mission, and that alignment with this mission is regularly reviewed.

2.2.2. Organizational Structure and Responsibilities

One of the key factors influencing the control environment is the organizational structure of the administration. Organizational structure provides a framework for the administration to achieve its objectives.

The organizational structures of public administrations are generally determined in the founding legislation prepared in accordance with the framework set out in Law No. 3046, and the administrative units (main units)

The duties of administrative units (service, advisory/supervisory, support units) are defined in these regulations. However, the duties of the sub-units of the administration are not included in these regulations but are determined by administrative regulations such as rules and directives.

The organizational structures of local administrations are shaped within the framework of the Municipalities Law No. 5393, the Metropolitan Municipalities Law No. 5216, the Provincial Special Administration Law No. 5302, and the Local Administration Unions Law No. 5355.

In order to create an appropriate control environment, the organizational structure of the administration must be structured accordingly.

- Showing the division of labor among administrative units within the organization,
- It should include accountability mechanisms and reporting channels to ensure the functioning of these mechanisms,
- Defining political responsibility, administrative responsibility, implementation-execution responsibility, control responsibility, and auditing and reporting responsibility within the framework of the principle of separation of duties,
- It is necessary to show the coordination, advisory and support units.

To meet the above-mentioned requirements, it would be appropriate to prefer a horizontal organizational structure that is dynamic, facilitates effective communication, and prioritizes participation and specialization.

On the other hand, it is important that the tasks of the units and subunits within the organizational structure are defined in a way that is consistent with the administration's mission. Therefore, it is necessary to ensure that the tasks of the units and subunits are aligned with the mission, and that the organizational structure and tasks are revised in line with these changes by continuously monitoring them.

2.2.3. Job Descriptions

As stated in the Public Internal Control Standards, the written definition of tasks to be carried out by the units and sub-units of the administration, and the creation of a task assignment chart that includes the duties of the personnel and their related authority and responsibilities, are important for the fulfillment of the administration's mission.

The process for preparing job descriptions within this framework is shown below. Public administrations They will be able to prepare job descriptions by following the process below.

KO Box 5: The Job Description Preparation Process

JOB ANALYSIS TO BE DONE



Job analysis is a process that involves gathering information about the nature of each job performed within an administration, as well as the environment and working conditions, and systematically examining and evaluating the collected data.

KEY QUESTIONS IN THE JOB ANALYSIS PROCESS

- What are the job requirements? (In terms of knowledge, skills, and experience)
- How is the work done? • When is the work done? • Where is the work done? • Why is the work done?
- What are the tools (hardware) that assist with the job?
- What kinds of outputs are obtained?



Job analysis alone is meaningless. It is only meaningful insofar as it contributes to the administration's achievement of its objectives. Therefore, the analysis must primarily contribute to the administration's goals.

It should begin with a thorough understanding of the organization itself, its philosophy, its mission and objectives, and the role and importance of each unit within the administration, and should continue in that direction.

The findings from the job analysis should be presented systematically and consciously, and the final job descriptions based on these findings should be approved by management.

Job descriptions for personnel should be prepared based on the job description of the unit in which the personnel will work. The job descriptions of personnel with the same title should vary depending on the unit they work in.

Job descriptions must include at least the following information:

- Units and sub-units
- Job title (position name)
- The title to which the position is attached
- Competency level (knowledge, problem-solving, areas of responsibility)
- Main duties and responsibilities
- Authorities
- Skills and abilities required for the job
- Relationship with other tasks •

Approval section and notification to personnel section

JOB ANALYSIS DATA DUTY/TASK DEFINITIONS CREATION

JOB DESCRIPTIONS TO THE STAFF NOTIFICATION

In order for personnel working in public administrations to understand what their duties are, the rules they work under, and their objectives, it is necessary to communicate job descriptions to all personnel.

JOB DESCRIPTIONS UPDATED

Job descriptions must be reviewed and updated at least once a year.

2.2.4. Sensitive Tasks

Some tasks performed in public administration are, by their very nature and due to factors such as the reputation of the administration, the risk of corruption, the disclosure of confidential information, and similar considerations, far more important than others.

Hassas Görevler

Bir görevin hassas olup olmadığı değerlendirilirken en az aşağıdaki kriterlerin dikkate alınması uygun olacaktır:

- İdarenin hedeflerini etkileyebilecek önemli kararları alma kapasitesi
- Kararları etkileyebilecek İdare dışı Üçüncü kişi ve kuruluşlarla ilişkisi
- Gizli bilgilere erişim
- Mali değeri yüksek olan iş ve işlemlerle ilgili görevler
- Görevin yüksek seviyede özel uzmanlaşma gerektirmesi
- İdarelerce ilave edilebilecek diğer kriterler

Administrations should identify sensitive tasks according to these criteria, develop specific control mechanisms (rotation, assignment of backup personnel, etc.) to mitigate the identified risks, and review changes in risk levels.

Table 1 lists the areas of activity that may be sensitive for administrations and the related issues. Examples related to the tasks are provided:

KO Table 1: Examples of Sensitive Tasks

Management Areas	Examples of Sensitive Tasks
Financial management	• Issuing a spending instruction • Accounting • Payment processing
Commitment process	• Membership of the tender committee • Preparation of the contract draft • Inspection and acceptance
Human resources management	• Job Description • Recruitment process • Performance evaluation • Implementation of the salary system
Information management systems	• Access to systems and controls • Security of systems and key documents
Support Services	• Control of valuable inventory

2.2.5 Monitoring Task Results

Managers direct the activities of their units through written or verbal instructions. However, due to the structure of the units, the complexity of the organization, the dispersed organizational structure, the large number of employees, the variety of tasks performed, and similar reasons, the assigned tasks

Monitoring the results can be challenging from a management perspective. To overcome this challenge, managers should develop various methods, such as reporting tools and regular meetings.

Administrations should continuously evaluate sensitive tasks and decide on necessary action steps based on changes in risk levels (such as updating controls while considering cost-effectiveness, identifying new sensitive tasks, and reassessing the risk levels of sensitive tasks).

2.3. PERSONNEL COMPETENCE AND PERFORMANCE

The third standard of the control environment aims to ensure efficiency, productivity, and effectiveness in operations by effectively managing human resources, thereby enabling the achievement of the administration's aims and objectives.

KO Box 6: People First



ÖNCE İNSAN

- **"İnsanı kazanan işinde de kazanır"** ilkesinden hareketle bir idaredaki çalışanların kalitesi o idarenin çıktılarının kalitesi demektir.
- Çalışanların önce insan olduğunu düşünmek ve idarenin ihtiyaçları ile çalışanların ihtiyaçları arasında bir denge kurmak gerekir.
- İlk işe alım sürecinden başlayarak emeklilik sürecine kadar her aşamada liyakat ve kariyerleri ile doğru orantılı görevlerin verilmesi kişisel motivasyon açısından çok önemlidir.
- Bir idarenin maddi olarak ölçülemeyen tek sermayesi insandır.

The primary objective here is to select, train, evaluate the performance of, and plan the careers of personnel suitable for fulfilling the administration's mission, ensuring they possess fundamental skills and sufficient knowledge while maintaining a high sense of belonging and responsibility in their activities.

2.3.1. Human Resources Management

Today, in the public sector, there is a need to systematically manage human resources, the most important asset of the institution, in order to increase efficiency. In this context, shifting from the classical personnel management approach, which focuses on necessary personnel recruitment and compensation, to Human Resources Management (HRM), which aims to generate efficiency and competitiveness through various mechanisms, is considered one of the most important elements of good management.

Senior management plays a crucial role in HR, as they are responsible for setting policies, goals, and standards. Senior management must also create a transparent and accountable environment that complies with regulations and the law.

At the same time, HR is the responsibility of all levels of management, starting from top management. In line with these policies, unit managers, while effectively performing the tasks assigned to them by senior management, must also undertake responsibilities such as onboarding and training new personnel, improving job performance, developing a suitable work environment and relationships that ensure collaborative work, maintaining high morale and motivation among personnel, monitoring their health and improving working conditions, and monitoring employee satisfaction.

2.3.2. Fundamental Elements of Human Resources Management

The fundamental elements of HRM can be listed as follows:

• <i>Conducting job analyses;</i>
Job descriptions
The requirements of that task
• <i>Human resources planning;</i>
Staff analysis
Cost-benefit analysis
Restrictions in various legal regulations (Central Government Budget Law, General (Decree Law on Staffing Procedures, etc.)
• <i>Recruitment process;</i>
SWOT analysis (of the recruitment process)
Advertisements in newspapers, on the internet, and on government notice boards.
Fair, non-discriminatory, easy and needs-meeting application methods development
The examination process should be transparent to all relevant parties in a way that inspires confidence.
• <i>Career development and merit system;</i>
Promotion/Success criteria
Personnel performance indicators
Career plans
those reward mechanisms
• <i>Training and development activities;</i>
Educational needs surveys
Training programs (theoretical and practical)
Overseas education and internships
end-of-training assessments
Participation in conferences, workshops, etc. that support personal development.
• <i>Low performance and disciplinary actions;</i>
The basis for the decision of unsuitability for the position should be determined, taking into account current legislation, and this should be communicated to all employees.
The criteria for termination of employment and duty should be clearly defined, taking into account the existing legislation, and these criteria should be communicated to the personnel.
• <i>Working Environment;</i>
Employee safety
Employee satisfaction
Employee health

Public administrations should develop their human resources policies taking into account the fundamental elements mentioned above; and implement methods, regulations, and practices appropriate to their organizational structure, in line with their aims and objectives.

2.4. DELEGATION OF AUTHORITY

Authority refers to which administrative authorities or bodies can make administrative decisions or take actions. or indicates that it can be done.

Delegation of authority means giving others the right to make decisions, take action, or issue orders on a particular matter. This can be expressed as delegating responsibility and holding the other party accountable for the consequences.

2.4.1. Delegation of Authority and Workflow Processes

In administrations, workflow processes for activities should be established in writing, and those involved in these processes should be defined along with their authority limits and responsibilities. These defined processes should be analyzed to determine which authorities should be delegated to whom.

In delegating authority, it is expected that the person receiving the authority is familiar with the process and possesses the necessary qualifications and experience to manage it. Employees should periodically report the current status of the processes to their superiors, and the person delegating the authority should request these reports.

2.4.2. Delegation of Authority and Responsibility

Responsibility, within the scope of administrative activities, refers to a person's own actions or those within their area of authority. It is the act of assuming responsibility for the consequences of any event. In delegation of authority, two types of responsibility can be mentioned:

•	Administrative responsibility refers to the hierarchical responsibility of a subordinate to a superior. Delegation of authority does not relieve the delegator of administrative responsibility.
•	Financial responsibility refers to the financial liability arising from the exercise of authority and resulting in damage to the state and/or individuals. If authority is delegated, the financial responsibility arising from the use of that authority will rest with the person exercising the authority.

2.4.3. Matters to be Considered in Delegating Authority

- Delegation of authority must be based on law. Delegation should only occur in cases explicitly permitted by law and limited to the specified subject matter.
- To ensure the rapid and efficient delivery of services and to allow management levels to focus on policy-making and monitoring functions, delegation of authority to lower levels should be encouraged in cases not explicitly prohibited by law. The risks arising from delegation of authority should be managed through hierarchical controls and an effective monitoring system.
- There are powers that cannot be delegated by law and are not at the discretion of the administration. The exercise of these powers is directly granted to a public official by law (for example, the power to make appointments, the power to impose disciplinary penalties).
- Delegation of authority must be done in writing.
- The limits of the authority to be delegated must be clearly defined.
- Delegation of authority should be done taking into account the importance of the delegated authority.
- Delegation of authority should be partial; it should not be done by delegating all authorities.
- Personnel to whom authority is delegated must possess the knowledge, experience, and skills required for the task.
- Personnel to whom authority is delegated must provide periodic information to the delegator regarding the use of their authority, and the delegator must monitor this process. To ensure this, standard reporting formats should be developed and used.
- As long as the delegation of authority continues, the person who delegated the authority will not be able to exercise that authority.
- The delegated authority cannot be delegated to another person by the delegated party.
- The delegation of authority is made to the office, not to the person. The authority is delegated to or received by the office. Even if the personnel changes, it will remain valid unless the delegation of authority is revoked.
- Authority cannot be delegated to more than one person on the same matter.

2.4.4. Delegation of Signature Authority

The delegation of signing authority means that the authorized body has the power to sign only certain parts of the transactions for which it is authorized. It is the act of delegating to subordinates.

When signing authority is delegated, the transferee exercises that authority on behalf of the delegating authority.

Furthermore, in cases where signing authority is delegated, the delegating authority may exercise this authority personally at any time. The delegation of signing authority must be done in writing and with sufficient clarity. The delegation of authority is made to an office, while the delegation of signing authority is made to an individual. Consequently, the delegation of signing authority ends when the person delegating or receiving the authority leaves their position.

PART TWO

RISK MANAGEMENT

1. INTRODUCTION

Governments use the resources allocated to them to achieve their aims and objectives. The decisions made, activities, processes, and projects carried out regarding the use of these resources also bring risks.

Risk management helps administrations achieve the goals they set in line with their vision and mission. It is a helpful tool. Risk definition is included in RY Box 1.

RY Box 1: Definition of Risk Management

- Events or situations that are assessed to potentially negatively affect the achievement of aims and objectives are defined as risks, while events or situations that are assessed to potentially have a positive impact on aims and objectives are defined as opportunities.
- Identifying and evaluating events or situations that are likely to occur and are assessed to affect the achievement of the administration's aims and objectives, and providing appropriate responses to these events, as well as all activities carried out on this basis, constitute the subject of Risk Management.

Risk management encompasses the stages of defining a risk strategy, identifying and evaluating risks, responding to risks, reviewing risks, and reporting risks. Risk management must be applied consistently throughout the entire organization, which gives rise to the concept of "Enterprise Risk Management." Enterprise risk management is a process that includes the entire organization. It ensures that risk management processes are viewed and managed as a whole.

2. RISK ASSESSMENT STANDARDS

Administrations, when implementing risk management, take into account the standards and general requirements related to these standards, as outlined in RY Box 2.

RY Box 2: Risk Assessment Standards



İdareler, faaliyetlerini, amaç, hedef ve göstergelerini ve bunları gerçekleştirmek için ihtiyaç duydukları kaynakları içeren plan ve programlarını oluşturmalı ve duyurmalı; faaliyetlerinin plan ve programlara uygunluğunu sağlamalıdır.

Bu standart için gerekli genel şartlar:

- 5.1** İdareler, misyon ve vizyonlarını oluşturmak, stratejik amaçlar ve ölçülebilir hedefler saptamak, performanslarını ölçmek, izlemek ve değerlendirmek amacıyla katılımcı yöntemlerle stratejik plan hazırlamalıdır.
- 5.2** İdareler, yürütecekleri program, faaliyet ve projeleri ile bunların kaynak ihtiyacını, performans hedef ve göstergelerini içeren performans programı hazırlamalıdır.
- 5.3** İdareler, bütçelerini stratejik plan ve performans programlarına uygun olarak hazırlamalıdır.
- 5.4** Yöneticiler, faaliyetlerin ilgili mevzuat, stratejik plan ve performans programıyla belirlenen amaç ve hedeflere uygunluğunu sağlamalıdır.
- 5.5** Yöneticiler, görev alanları çerçevesinde idarenin hedeflerine uygun özel hedefler belirlemeli ve personeline duyurmalıdır.
- 5.6** İdarenin ve birimlerinin hedefleri, spesifik, ölçülebilir, ulaşılabilir, ilgili ve süreli olmalıdır.

6. Standart

**Risklerin Belirlenmesi
Ve Değerlendirilmesi**

İdareler, sistemli bir şekilde analizler yaparak amaç ve hedeflerinin gerçekleşmesini engelleyebilecek iç ve dış riskleri tanımlayarak değerlendirmeli ve alınacak önlemleri belirlemelidir.

Bu standart için gerekli genel şartlar:

- 6.1** İdareler, her yıl sistemli bir şekilde amaç ve hedeflerine yönelik riskleri belirlemelidir.
- 6.2** Risklerin gerçekleşme olasılığı ve muhtemel etkileri yılda en az bir kez analiz edilmelidir.
- 6.3** Risklere karşı alınacak önlemler belirlenerek eylem planları oluşturulmalıdır.

3. BENEFITS THAT RISK MANAGEMENT CAN PROVIDE TO THE ADMINISTRATION

The main benefits that risk management can provide to management can be expressed as follows:

- To contribute to the administration's achievement of its aims and objectives and to improve its performance,
- To help ensure the continuity and improve the quality of services provided and activities carried out by administrations,
 - To increase efficiency in resource allocation by

using benefit-cost, cost-effectiveness, or other necessary analysis methods in risk management,

- Keeping the effects of potential losses under control and the costs they will cause to contribute to its reduction,
- To ensure compliance with legislation and regulations,
- Strengthening decision-making mechanisms through an evidence- and risk-based approach to ensure,
- Increasing accountability by supporting the clear definition of duties, authorities, and responsibilities related to the risks of the administration,
- To contribute to administrations having a more positive image in the public eye.
- To increase employees' sense of ownership and belonging.

4. CRITICAL SUCCESS FACTORS FOR EFFECTIVE RISK MANAGEMENT

In order for administrations to achieve the expected benefits from risk management: •

The risk management process should be embraced by top management, and a risk strategy should be created and implemented in line with the vision and mission,

- Establishing the necessary mechanisms to have a common and consistent risk management language,
- Providing adequate information, guidance, and advice on risk management,
- Risk management processes should be simple, flexible, and implementable, and planned and executed in an integrated manner with other essential processes (strategic planning, performance management, human resources management, etc.), • Risk assessments

must be supported by reliable evidence,

- Systematic monitoring, reporting, and evaluation of risk management processes,
- Establishing within management an awareness that everyone has an important role in the risk management process and that risk management should be carried out as an integral part of existing activities, • Having a defined corporate communication strategy and appropriate communication within and outside the management. creation of channels,
- What is important in risk assessment is not the techniques applied, but rather who will assess the risks. taking into account the experience and knowledge of those involved, is required.

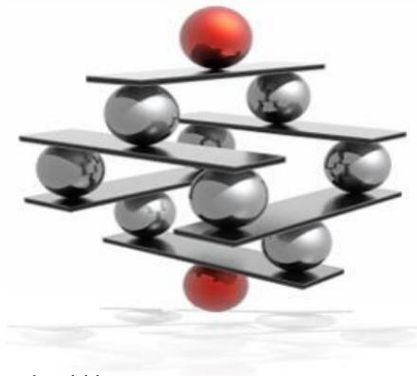
5. Risk Management Strategy

The corporate approach and high-level policies regarding risk management are called Risk Management Strategy; this The document in which these approaches and policies are set out in writing is called **a Risk Strategy Document (RSD)** .

The risk strategy reflects the administration's approach to risks and provides a framework for the risk management process. The Risk Management Statement (RSS), prepared by the administration's Internal Control Monitoring and Steering Committee, must be approved and announced by the senior management and made accessible to all employees.

While preparing the RSB, the following was included under heading 4 of this section: Critical success factors must be considered.

The risk strategy should be defined in a way that reflects the administration's risk appetite at a strategic level. Since risk appetite can change over time depending on circumstances, the administration's risk strategy should be...



It should be reviewed at least once a year and updated as necessary.

RY Box 3 covers key aspects related to risk appetite.

RY Box 3: Risk Appetite

- **Risk Appetite; is the highest level of risk that the administration is prepared to accept (tolerate/be exposed to/ not take precautions against) in line with its objectives. The concept of risk appetite implies that risks above this level are unacceptable and require precautionary measures.**
does.
- **The current R&D policy is also taken into consideration when preparing the Strategic Plan.**
- **Risk appetite is influenced by the internal and external environment, people, and policies. Within this context, risk appetite is determined from top to bottom at the institutional/unit/subunit levels, as part of the Risk Management Strategy.**
- **Provided that the risk appetite limits set by the administration at the institutional level are maintained, it is possible for units/subunits to determine different levels of risk appetite.**
- **Just as taking too much risk can lead to failure, so can taking too little risk. While a low risk appetite is seen as a reliable management technique, it can limit creativity, innovation, and the ability to seize opportunities.**

The corporate risk strategy should be determined taking into account the above explanations and should be consistent with higher-level policy documents. The Risk Assessment Report (RSB) should include the minimum elements listed in Box 4 of the Risk Assessment Report. Administrations may also include information they deem necessary in the RSB, depending on their organizational structure. The general international approach is that the RSB should be prepared every three (3) years and revised annually.

RY Box 4: Minimum Requirements Deemed Suitable for Inclusion in the RSB

- **The purpose of Corporate Risk Management**
- **Risk Appetite Level**
- **Risk methodology to be applied**
- **Risk categories**
- **Risk identification criteria**
- **Risk assessment criteria**
- **Organizational structure and tasks related to risk management.**
- **To what level will the risks be managed (such as unit/subunit/regional units)***
- **Frequency and procedures of meetings and reporting.**
- **The role and contribution of employees to risk management.**
- **Document formats to be used**
- **Strategies and methods to be applied in control activities**

**It would be appropriate for administrations to manage risks at the administrative (strategic) and unit levels in the initial stages, and then gradually include sub-units and regional units in the scope based on the experience gained.*

6. DUTIES, POWERS AND RESPONSIBILITIES

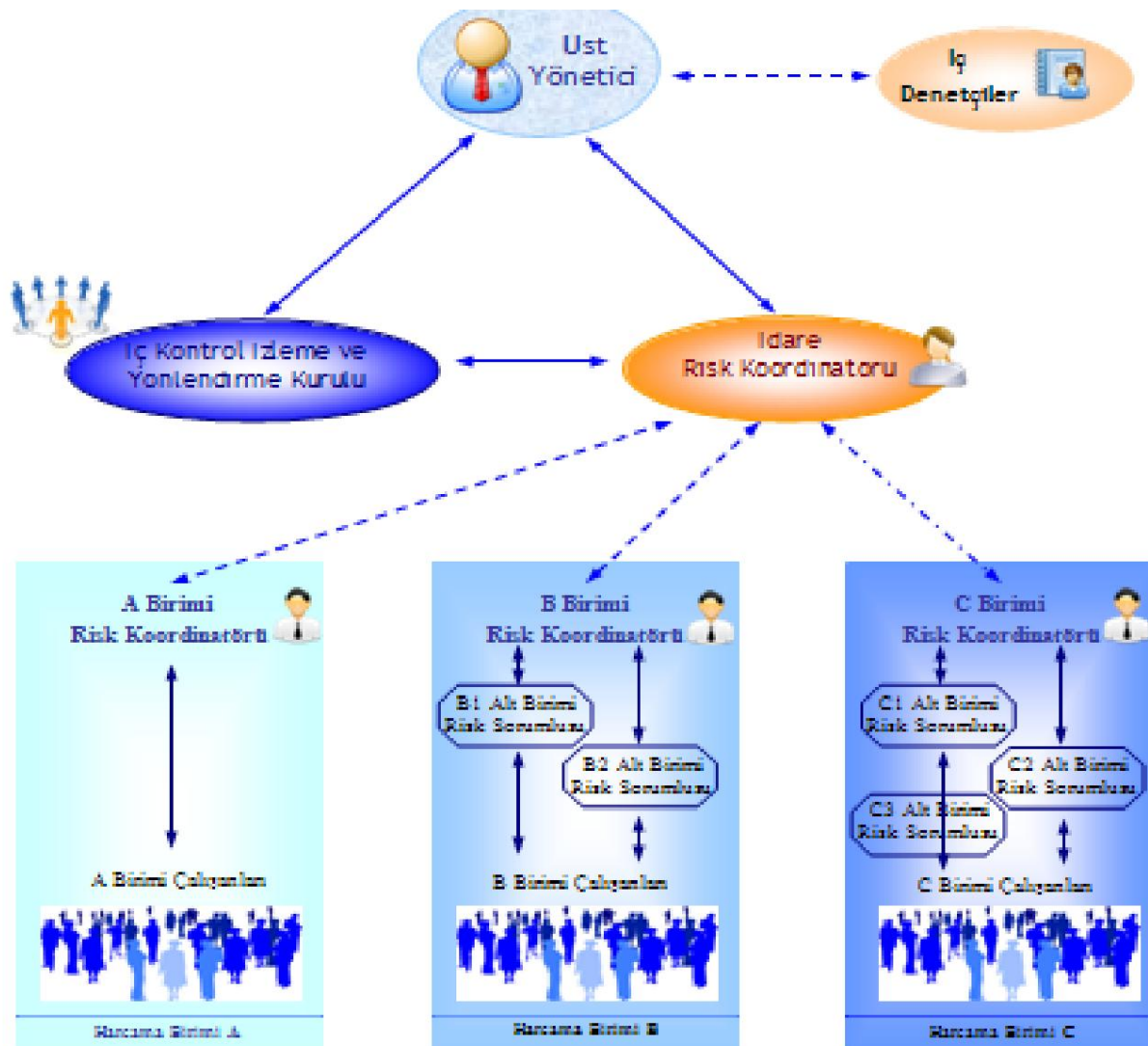
Effective risk management is possible with a well-organized administration.

This requires clear definition of roles, authorities, and responsibilities within the administration, a clear understanding of what is expected of individuals within the context of the administration's policies and practices, and the existence of a suitable communication mechanism for horizontal, vertical, and external communication.

Assigning tasks and responsibilities in risk management to appropriate, competent, and authorized individuals will create a strong infrastructure for the administration's risk management efforts.

Figure 1 of RY shows the structure regarding duties and responsibilities in risk management within the administration. Administrations are required to identify appropriate personnel to perform the functions listed in the diagram below, within the framework of their organizational laws and structures.

Figure 1: Roles and Responsibilities in Risk Management



6.1. Senior Management

Within the framework of Law No. 5018, the top-level executive with the highest authority and responsibility also leads their administration in risk management.

Senior executive in risk management;

• Every three years, the management ensures the development of a strategy for managing risks in line with its aims and objectives, approves the Risk Management Statement (RSB) showing how this strategy will be implemented, and communicates this document in writing to all employees.
• RSB establishes the necessary structures (such as the Internal Control Monitoring and Steering Committee (ICMS)) for risk management within the scope of this Guideline, and clearly defines the duties and responsibilities.
• Provides the necessary support to the Administrative Risk Coordinator (IRC) regarding risks that need to be managed jointly with other administrations.
• Showing the necessary sensitivity and participation in managing risks to stakeholders and the public. It ensures that appropriate mechanisms are established to provide this.
• Based on the assessments and recommendations provided by IKIYK and IRK, it determines strategic actions for the future.
• It obtains assurances from the IKIYK (Internal Control and Supervision Agency) and the internal audit unit regarding risk management and submits evidence to the minister, or to the relevant council in local administrations, regarding whether risks are effectively managed within its administration.
• It ensures the consistency of risk management processes.
• Reviews monitoring reports and ensures the effectiveness of risk management.
• They demonstrate exemplary behavior, especially in managing strategic risks.
• It incentivizes employees at all stages of risk management.

6.2. Internal Control Monitoring and Steering Committee (ICMS)

The Risk Management Committee (RMC), chaired by a senior deputy manager or unit manager and composed of unit managers or their designated deputies, develops policies and procedures for improving the administration's risk management and submits them to the senior manager for approval.

It communicates policies and procedures to the units. The IKIYK takes into consideration the risks that it deems strategically important from among the risks presented to it by the IRK.

The secretariat services of the IKIYK are carried out by SGB. Meetings are convened when deemed necessary. Experts from within or outside the administration may be invited.

Regarding risk management, IKIYK;

• Prepares the administration's Risk Management Statement (RSS) and submits it to the senior management for approval. • Establishes policies for creating a risk management culture within the administration.
• It ensures that risks are managed consistently within the organization.
• Risks belonging to spending units that need to be managed jointly, and the policies related to them. It notifies IRK in order to coordinate by defining the procedures.
• It identifies risks that need to be managed jointly with other administrations and reports them to the IRK, ensuring that necessary measures are taken for joint management with the relevant administrations.
• The IKIYK (Internal Control and Prevention Board) meets at the frequency they have determined in the RSB (Risk Management Board) to ensure that the administration's risk management processes are functioning effectively. They report to senior management that the process is not working and assess the current situation regarding the risks.
• It supports the identification and dissemination of best practice examples by utilizing reports from the Court of Accounts and internal audit reports.

6.3. Administrative Risk Coordinator (IRC)

The senior manager designates one of their assistants or the SGB manager as the IRC (Internal Control Point). The IRC is a natural member of the IKIYK (Internal Control Point) and is accountable to the senior manager for the implementation of the administration's risk management processes.

Regarding risk management, IRC;

- As part of risk management, it convenes a meeting of the Unit Risk Coordinators (BRK).
- Based on the unit risks reported by each BRK, it prepares the Consolidated Risk Report (RY Appendix 4); it submits this report to the IKIYK and senior management at the specified periods. Along with this report, it also reports the important risks that need to be monitored and its own assessments.
- Responsible for discussing issues related to shared risk areas with the IRCs of other administrations and coordinating these within the administration.
- Identify the risk management needs of the units and present this before each meeting.
Reports to IKIYK.
- Provides feedback to BRKs regarding the opinions, recommendations, and decisions of the IKIYK and assesses the administration's risks. It takes the necessary measures to ensure consistency in management processes.

6.4. Unit Risk Coordinator (BRK)

The Internal Control Committee (ICC) is selected by the unit manager from among individuals who have experience and expertise in the unit's duties and internal control practices. However, in administrations where appointing an ICC is difficult due to factors such as small organizational structure and insufficient personnel, the unit manager may act as the ICC.

BRKs in risk management;

- Coordinates and provides guidance in identifying risks that could affect the unit's objectives.
It matches identified risks with the activities of its sub-units by leveraging their knowledge and expertise, and ensures that all key issues are addressed.
- The unit reviews the annually determined risk records and related reports at intervals determined by the administration (such as monthly or quarterly) and reports them to the IRC (Insurance Coordination Center) with the approval of the unit manager.
- Monitors the risks reported by Sub-Unit Risk Coordinators (SUCs) at the unit level. Evaluates changes in existing risks and any new risks, and reports them to the Internal Control Committee (ICC) after obtaining the unit manager's approval.
- On an annual basis, it submits evidence to the IRC on whether previously identified risks or risks that may arise during the year have been well managed.
- Feedback to ARKs, if any, in line with the opinions, recommendations, and decisions of IRC and IKIYK.
provides.
- Identifies training needs related to risk management.

6.5. Sub-Unit Risk Coordinator (ARK)

In administrations where risk management at the sub-unit level is deemed appropriate, the Risk Management Representative (ARK) is the sub-unit manager or their designated representative. The ARK is responsible for coordinating risk management activities at the sub-unit level.

In risk management, ARKs (Armed Forces)

- involve:** • Identifying, evaluating, responding to, and reviewing risks at the sub-unit level.
It coordinates the performance of tasks such as monitoring and reporting.
- In accordance with the administration's risk strategy, the sub-unit reports to the BRK, at intervals determined by the BRK, newly identified risks related to its activities, those whose risk scores have changed, and the effectiveness of the controls used to mitigate these risks.
- They are also obligated to provide the information and documents requested by the IRC.

6.6. Employees

The success of risk management depends on employee ownership of it. Therefore, each employee is responsible for managing risks (identifying, assessing, responding to, reviewing, and reporting risks) within their area of responsibility.

Those working in risk management;

- | |
|---|
| <ul style="list-style-type: none"> By identifying, communicating and responding to newly emerging and changing risks. They directly contribute to risk management processes within their units. |
| <ul style="list-style-type: none"> Managing the risks in the area of responsibility, within the scope of the authority and responsibilities determined by the administration.
He/She manages. |
| <ul style="list-style-type: none"> Provides ARK with the necessary evidence regarding whether the risks in the area of responsibility are being managed effectively; if ARK is not available, it provides BRK with the necessary evidence. |

Employees should not hesitate to identify risks and report them to the relevant risk coordinator.

6.7. Internal Audit Unit

The internal audit unit reviews whether the risk management process is effective and whether risks are managed appropriately, and prepares the necessary reports for senior management within the framework of the legislation. Administrations can benefit from the consulting services of internal audit units, such as facilitation and training, in establishing and developing the risk management process.

6.8. Strategy Development Units

- | |
|--|
| <ul style="list-style-type: none"> It coordinates risk management activities within the administration and, as part of the evaluation of the internal control system, assesses the effectiveness of risk management and reports to the Internal Control Management Board on a periodic basis. |
| <ul style="list-style-type: none"> Technical measures to ensure that risk management processes function effectively in all units of the administration. It provides support and guidance services. |
| <ul style="list-style-type: none"> Identifying training needs related to risk management, conducting training activities, and is responsible for coordinating |
| <ul style="list-style-type: none"> Identifies best practices in risk management within the administration and works to disseminate these practices. |
| <ul style="list-style-type: none"> If the IKIYK and SGB manager are not IRK, IRK will carry out the secretariat services. |

6.9. Central Harmonization Unit of the Central Executive Committee (CEC)

MYK MUB makes regulations in the field of internal control, including risk management. In line with national and international best practices, it develops standards and methods related to risk management, and carries out training, guidance, harmonization, and reporting activities.

7. RISK MANAGEMENT PROCESS

Corporate Risk Management (CRM) is a management tool aimed at providing reasonable assurance that an administration can achieve its aims and objectives. In this context, administrations need to carry out CRM activities simultaneously with the preparation of strategic plans and performance programs. Administrations first establish a balance between the objectives and risks that will enable them to achieve the aims stated in the strategic plan, and determine their targets within the framework of the risk appetites determined by the RSM.

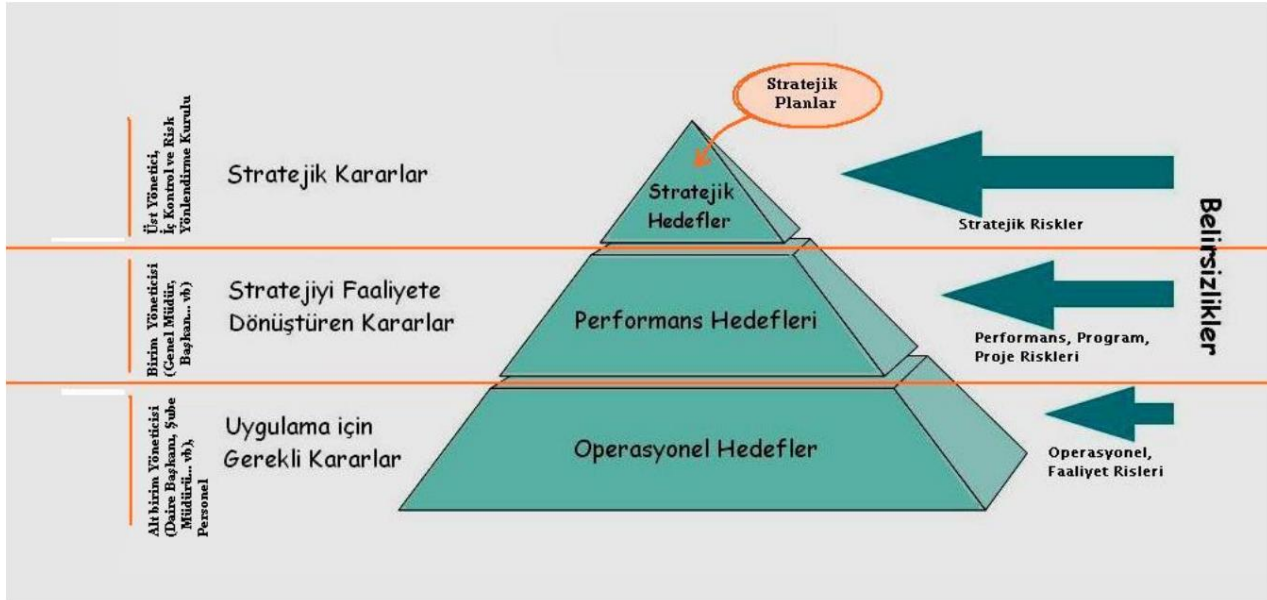
* In administrations that already have strategic plans in place, the risk management process should be initiated as soon as possible.

** In administrations that are not required to prepare a strategic plan and performance program, the risk management process is defined as Risk Management System (RSB). It begins with defining management aims and objectives within the framework of their interests. Strategic risks are also identified at this stage.

The risk management cycle is considered throughout all stages of the strategic plan preparation phase, starting with the setting of objectives and ending with the analysis of whether the objectives have been achieved as intended.

Administrations should manage risks at the strategic, unit, and activity levels, as shown in Figure 2 of the RY.

RY Figure 2: Risk Hierarchy



Administrative level (strategic level): This is the area encompassing the entire administration, where decisions regarding strategic objectives are made, and which is the responsibility of the administration's top management. Strategic objectives are oriented towards the medium and long term and are linked to high-level policy documents. Therefore, when making decisions about the future, decision-makers (top management) must consider a great deal of uncertainty. This is the area where the impact of risks is highest; it is most affected by external risks such as government policies, the general economy, and technological developments. Risks that are not well managed at the strategic level are of particular importance because they will affect other levels as well. The top management is responsible for managing the risks that need to be managed at the strategic level.

Unit level (program/project level): This refers to the units where top management policies are implemented and where the highest level of responsibility for the use of public resources within the administration is held. Risks at this level have a shorter-term impact compared to strategic risks. It is the area where the unit must define its own functional objectives and manage the risks related to these objectives in order to achieve the administration's strategic goals. It is affected by risks originating both externally and internally. Because it requires the assessment of risks from both lower and upper levels and necessitates good coordination with units operating in different areas towards the same strategic goal, it is of key importance. The unit manager is responsible for managing the risks that need to be managed at the unit level.

Sub-unit/Provincial unit level (activity level): Activities carried out at this level are solely focused on achieving unit objectives. All employee activities fall within this scope. This is the area where short-term decisions are made, public services are provided, and uncertainties are minimized. It is more affected by internal risks than external risks. Poor risk management at this level negatively impacts the achievement of unit objectives and, consequently, strategic objectives.

Figure 3 illustrates the basic stages of the risk management process. Accordingly, the risk management process consists of the stages of identifying risks, evaluating risks, responding to risks, reviewing risks, and reporting risks. The responsibility for managing risks at the sub-unit/regional unit level lies with the sub-unit/regional unit manager.

Figure 3: Risk Management Process



7.1. Identifying Risks

Risk identification, the first stage of the risk management process, is the process of determining, grouping, and updating risks that hinder or complicate the achievement of the administration's objectives, using predefined methods.

RY Box 5 contains questions that administrations can consider when beginning to identify risks.

RY Box 5: Questions to Consider When Beginning to Identify Risks

- What are the main objectives?
- What are the key activities?
- Who are the stakeholders?
- What are our risk categories?

The following points should be considered when identifying risks:

- Administrations can initiate the risk management process by adopting a top-down approach to identifying risks, or a bottom-up approach, or by applying both methods simultaneously.
- Administrations identify their risks at the administrative (strategic), unit (program/project), and sub-unit (activity/operational) levels. • As a general rule, strategic risks that may affect the administration are identified during the strategic plan preparation phase. It is detected.
- Within the framework of strategic aims and objectives, units and sub-units also determine their annual targets and identify the risks related to them. Strategic considerations are taken into account when determining risks at the unit and activity level.

Risks are taken into consideration. However, when identifying unit and operational risks, it is important to think broadly, not just limiting oneself to the strategic level.

- When identifying administrative risks, the administration can choose a hierarchical approach, either top-down or bottom-up. Depending on the administration's preference, both methods can also be used together.
Initially, it would be beneficial to identify risks from a bottom-up perspective (from operational level to strategic level) in order to create a risk catalog containing all identified risks related to management and to increase employee ownership of risk management.
- Identified risks should be linked to objectives. However, it should be considered that some risks may affect objectives indirectly rather than directly. For example, damage to corporate reputation, or negative impacts on groups not directly identified as stakeholders as a result of the activity. Risks should be identified systematically and according to predetermined methods. These methods may vary depending on the characteristics of the administration and activities. In this process, one or more of the methods listed below can be used, or administrations can develop new methods according to their own needs.
- Identified risks should be expressed as "risk x" or "risk of x occurring". It is appropriate to record this in the Risk Registration Form as well (See RY Appendix 3: Risk Registration Form).
- Identified risks should be grouped by evaluating whether they are internal or external risks. • **Internal risks** are risks arising from events that can be directly controlled by management. Internal risks are further divided into three levels: strategic risks, unit risks, and operational risks.
They should be classified.
- **External risks** are risks that arise as a result of events outside the control of the administration.
It would be useful to classify and identify external risks according to their nature. After identifying the risks, it should be determined who is responsible for them and recorded in the Risk Record Form.
This information should be included.
- Risk management is a dynamic process, therefore, in addition to changes in existing risks, new risks are also needed. Potential risks must also be continuously monitored.

RY Box 6: Factors and Methods to Consider in Risk Identification

How can I identify the risks?

- **Decide whether you will identify risks first at the strategic level, at the operational level, or using a combination of both.**
- **Decide on your working methods.**
- **Group risks as internal and external risks. • Identify and group risks by considering threats or opportunities (economic, social, etc.).**
cultural, political, technological, legal, ethical, environmental, etc.).
- **Conduct a stakeholder analysis (determine the positions and attitudes of stakeholders).**
- **Regularly and during specific periods (elections, economic crises, natural disasters, etc.)**
Repeat the detection.

The following methods are commonly used to identify risks. However, these...
In addition, administrations may determine different methods according to their needs.

PESTLE Analysis (See RY Box 7)

SWOT Analysis (See RY Box 7)

Brainstorming (This method can be used for both identification and evaluation (See.

APPENDIX 1).

RY Box 7 includes PESTLE and SWOT analyses.

RY Box 7: PESTLE and SWOT Analysis

PESTLE Analysis

Risks are identified by evaluating them based on the following categories.

Politic ÷ Politics

Economic ÷ Economic

Social ÷ Social

Technologic ÷ Teknolojik

Legal ÷ Lawful

Environmental ÷ Environmental

Example:

Political	Risk of a shift in government priorities .
Economic	: The risk of the inflation rate being higher than expected.
Social	The risk of the population growth rate exceeding expectations significantly .
Technological	Risk of not establishing an IT infrastructure .
Legal	: The risk of complexity in the regulation of the relevant area.
Environmental	: The activity poses a risk of causing environmental pollution.

SWOT Analysis (Internal analysis)

Strengths ÷ Powers

Weaknesses ÷ Weaknesses

Opportunities ÷ Opportunities

Threats ÷ Threats

Example:

Strengths ÷ Competent staff
Weaknesses ÷ Outdated technology
Opportunities ÷ Economic growth
Threats ÷ Sudden policy change

For more detailed information, see: Ministry of Development, Strategic Planning Guide for Public Administrations, June 2006.

RY Boxes 8 and 9 contain tips and questions that can be used to identify risks.

RY Box 8: Tips for Identifying Risks

- In addition to the identified risk, the existence of evidence related to the risk is also taken into consideration. should be included.
- A working team comprising different areas of expertise to identify new risks increases the probability.

RY Box 9: Questions That May Be Asked During the Risk Assessment Process

• What could go wrong on the way to achieving our goals? •

What are our critical processes?

• Who are our stakeholders, and what might be their impact on our operations, or the impact of our operations on our stakeholders? • What are our risk

categories? • What are our weak

points? • Which of our assets are critical?

• What are the potential areas of irregularities and corruption?

• Under what circumstances or events might our operations be disrupted? •

What are our most critical information sources?

• What are the areas where we spend the most money?

• Which activities or processes are more complex?

• What are the legal requirements?

• What are the resource constraints?



7.2. Risk Assessment

Risk assessment involves analyzing the factors that could affect the administration's ability to achieve its objectives and evaluating the significance of the risk in terms of impact and probability.

When assessing risks, the specific circumstances of the administration (e.g., its size, the complexity of its operations, the legislation it is subject to, and the large number of people benefiting from its services) should be considered along with the potential events it may encounter.

Risk assessment involves measuring, prioritizing, and identifying risks after they have been identified. It includes the stages of recording.

Measurement is the calculation of the probability and impact of each risk. Prioritization is the process of measuring risks. The result is a ranking of individuals according to their importance based on the scores they received.

The recording of risks involves numbering each identified risk and having it recorded by authorized personnel. It involves approval and registration through forms determined by the administration.

Risk assessment involves determining whether and how to respond to the identified risks. If compensation is to be given, it helps in choosing the most appropriate compensation in terms of benefit/cost balance.

RY Box 10 contains some questions to consider when beginning a risk assessment.

RY Box 10: Questions to Consider When Beginning a Risk Assessment

- What are the goals?
- What are the existing controls?
- What are the potential consequences for the objectives if the risk materializes?
- Does the activity of another administration/unit affect our risk?
- Who are our stakeholders?

There are three key stages to assessing risks;

1- Measuring risks:**a) Determining the impact and probability of occurrence for each risk.**

• The **probability** and **impact** of the identified risks are measured. • **Probability** refers to the likelihood of an event occurring within a specific time frame. • **Impact** refers to the effect of this event, if it occurs, on the administration's goals and activities. It expresses the result it will create.

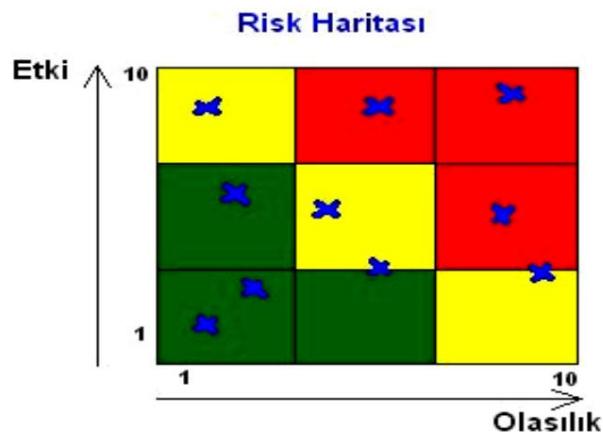
• The probability and impact of risks are shown numerically.

• For **probability**, the number 1 means that the probability of a risk occurring is almost zero; the number 10 means that the probability of the risk occurring is almost certain.

• In terms of **impact**, a score of 1 means the consequences of the risk's realization are of little importance; a score of 10 means the consequences are very important. The value of the risk on a scale of 1 to 10 in terms of probability and impact is determined (See: RY Appendix 5 Sample Risk Assessment Criteria Table, See: RY Appendix 2 Risk Rating Form). • The administration should consider risk appetite at this stage. Based on the determined risk strategy, the administration should identify which risks are low, which are medium, and which are high, and create its risk map accordingly (See RY Figure 4 Risk Map).

• A **three-part category** is used when assessing risks : low risk level (indicated in green), medium risk level (indicated in yellow), and high risk level (indicated in red). • The color coding of risks makes it easy to see the severity of the risk. It helps.

Risk maps are used to more easily visualize the level of risk . The values assigned to the risks represent the risk level. The simplified representation of RY on the map is shown in Figure 4.

RY Figure 4: Risk Map

b) Assessment of risks based on natural risk and residual risk:

• **Natural risk** is any risk that an administration identifies in relation to its objectives.

It indicates the level before a response is given.

Residual **risk** refers to the risks remaining after management has taken measures to reduce the probability and impact of a risk. Management must determine the level of residual risk after its response to managing the risk. If the level of residual risk is higher than the acceptable risk level, the effectiveness and adequacy of the risk response methods should be questioned, and if necessary, the responses to the risks should be reviewed again.

RY Box 11: Natural and Residue Risk Example

Strategic Objective 1. To lead the way in defining sustainable fiscal policies through a holistic approach and managing resources based on the 3Es (Economic, Social, and Economic) principle.

Strategic Objective 3: To streamline resource allocation and utilization processes while ensuring fiscal discipline and sustainable growth.

Performance Objective: To improve the financial management and control tools of public administrations and to increase the effectiveness of the monitoring and evaluation system in public financial management.

Activity: To conduct an Assistant Financial Services Specialist examination in order to strengthen the administrative capacity of the strategy development units of public administrations.

- Exam Procedures

Collecting those **requests**

Exam **preparations** (protocol with ÖSYM, announcement text, web infrastructure, etc.)

The **written and oral exams** and the placement process

The natural and residual risk assessment for the case study given above will be as follows:

Process: Gathering requests

Natural Risks: Failure of the request collection letter to reach the administrations, failure of the administrations' requests to reach our Ministry, and requests being made without a staffing quota.

Responses to Risk:

1. The request letter should also be sent by fax and published on the website.
2. Requesting that the administrations also send their application letters by fax.
3. Comparing the requests of public administrations under central government control with their staffing tables using the relevant unit records of the Ministry of Finance (*staffing information for local administrations is not available at the Ministry of Finance*).

Residual Risk: Including positions for local administrations that request positions even though there are no vacant financial services specialist assistant positions in the exam announcement.

2. Prioritizing Risks

- After determining the risk score, risks are ranked according to their importance, starting from the highest score. However, management may prioritize risks that directly affect objectives (key risks), even if they have a low score, due to their impact.
- Prioritizing risks according to their severity ensures efficiency in resource allocation.
- After identifying the risks in order of priority, decisions are made regarding the responses to those risks.

3- Recording Risks

- Recording risks provides evidence for decisions made and helps individuals participate in risk management. It helps them see and monitor their responsibilities.
- Risk records consist of two stages: **the Risk Record Form** (see RY Appendix 3), used for identifying and recording risks, and **Consolidated Risk Reports** (see RY Appendix 4), used for reporting risks to higher-level management.

RY Box 12 contains some tips for risk assessment.

RY Box 12: Tips for Risk Assessment

- **Measure the probability and impact of the identified risks over a specific time period.**
- **When determining the risk impact score, the objective that is expected to be difficult/impossible to achieve should be considered. Evaluate its impact.**
- **Keep in mind that the person doing the job is best positioned to assess its risks.**
- **The activities of other administrations/units may affect your risks, and the risks may differ from one another. Consider that it is not independent.**
- **Use risk maps or similar tables to see all risks together.**
- **Prioritize risks based on their risk scores (Impact x Probability) or their level of importance.**

RY Box 13: Example of Risk Assessment

EXAMPLE

You need to provide training related to your area of expertise.

Your goal: For your audience to understand the topic you are discussing.

You have identified your risks:

Risk 1: Being late for the training (and therefore not having enough time to explain what needs to be said)

Risk 2: Failure to properly determine the content (not knowing the target audience).

Risk 3: Forgetting the USB drive containing the presentation (reduced visual impact and perception)

Let's look at the probabilities of Risks 1, 2, and 3 occurring and how they would affect your goal if they did happen:

RISK 1:

Impact: You might be late, but you know the subject very well. Even if you explain it briefly, it will be understandable to the audience.

The impact of being late on your goal: 3

Probability: Traffic is heavy at that time. Also, you have other things to do that day. Chance of occurrence: 7

Risk Score: $3 \times 7 = 21$

RISK 2:

Impact: If you are explaining the topic to experts who know the subject, you need to explain it in detail; if you are explaining it to someone who knows nothing about it, you need to explain it in general terms. The impact of presenting with the wrong approach on your goal: 9

Probability: The assignment letter specifies the topic, but doesn't specify who you're supposed to explain it to. Chance of occurrence: 5

Risk Score: $9 \times 5 = 45$

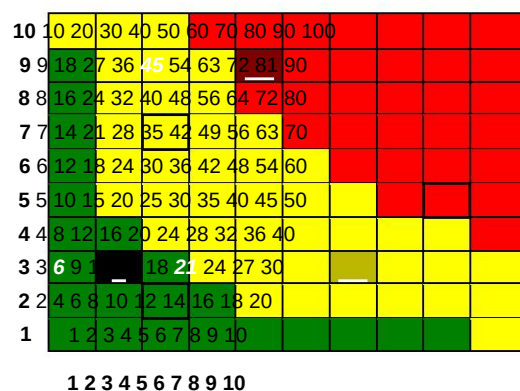
RISK 3:

Impact: Even without a presentation, you know the subject very well. You can explain it effectively to the audience. The impact of not giving a presentation on your goal: 3

Probability: You usually keep your computer with you at all times. You also have a habit of putting your work in your bag on a portable memory device. Chance of occurrence: 2

Risk Score: $3 \times 2 = 6$

Let's show it on the Risk Map:



Possibility

Let's prioritize:

1. Risk 2 (Risk Score: 45)
2. Risk 1 (Risk Score: 21)
3. Risk 3 (Risk Score: 6)

It's also important to note that risks shouldn't always be assessed based on scores. Some strategic risks, even with very low scores, must be considered. Emergency action plans should be in place. You can't always predict what will happen. Your plans must be flexible and able to cope when the unexpected occurs.

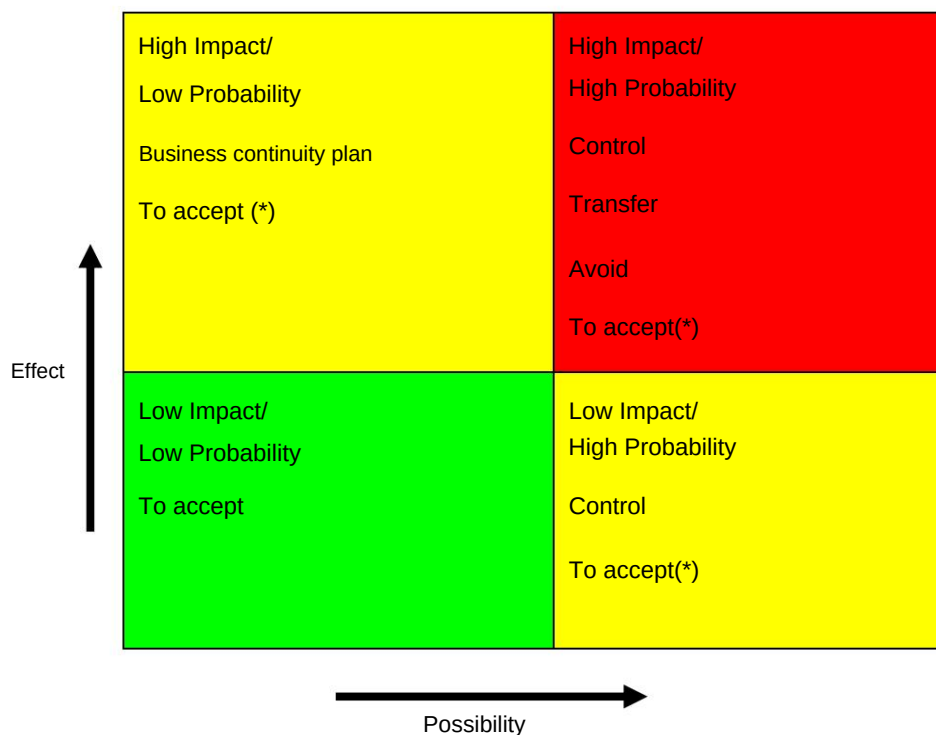
7.3. Responding to Risks

Responding to risks involves determining how to respond to risks identified by administrations and evaluated within the framework of risk appetite, and in this context, mitigating expected threats and/or evaluating emerging opportunities.

Before determining how to respond to risks, it is essential to conduct a cost-benefit analysis.

The aim of responding to risks is to achieve the intended goal in the most effective way by reducing the probability and/or impact of the risk. Figure 5 provides information about the responses to be given after evaluating the impact and probability of risks.

Figure 5: Risk Assessment and Response Matrix



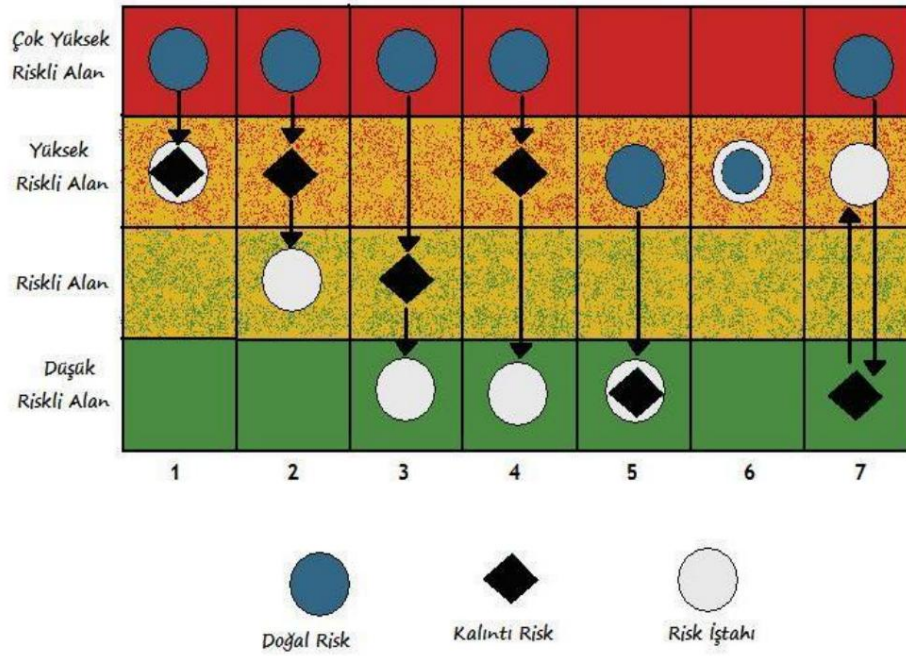
**See: "Accept" option*

RY Box 14: Questions to Consider When Responding to Risks

- What happens if I accept the risk?
- Which risks need to be controlled?
- Someone who can perform the activity better within the framework of cost-effectiveness analysis.
Is there an administration/business/organization?
- To avoid risk, postpone the activity to another period or find an alternative.
How does substituting with another activity affect my goals?
- Is the magnitude of the opportunity worth the risk?

Figure 6 illustrates how natural risk is transformed into residual risk as a result of the response to that risk, within the framework of risk appetite (See Box 3: Risk Appetite).

RY Figure 6: Risk Appetite Table



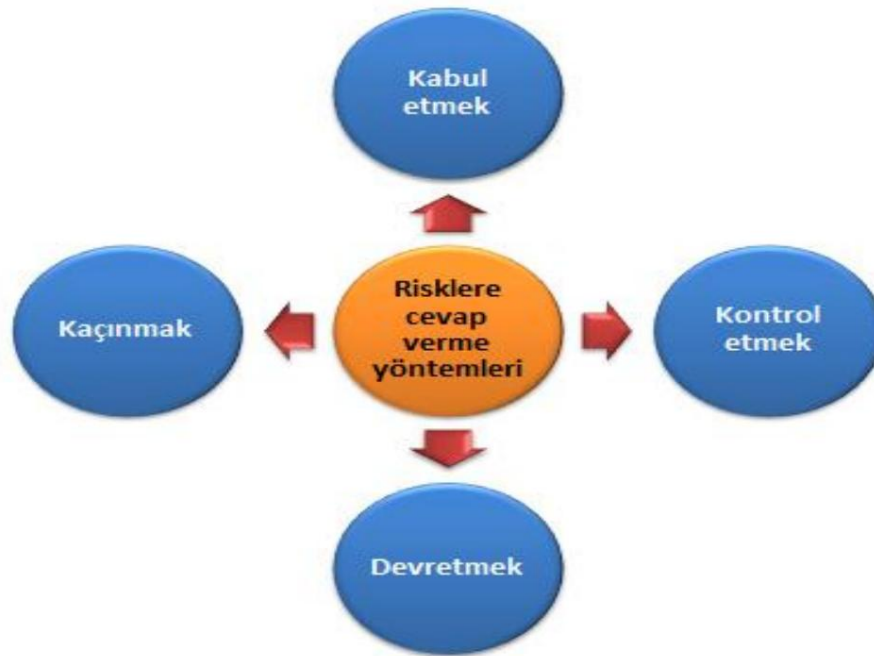
Source: This information was obtained from the Office of Government Commerce's Risk Dashboard/Thinking About Risk publication. United Kingdom HM Treasury

RY is shown in Figure 6;

- In columns 1 and 5, the response to risk reduces the inherent risk, thus lowering the residual risk to the same level as the risk appetite. These points where the administration's risk appetite and the residual risk intersect are ideal situations for risk management.
- In columns 2, 3, and 4, the response to the risk has reduced the risk. However, the residual risk is still higher than the risk appetite (acceptable level). This means that the effectiveness and adequacy of the response to the risk should be questioned, and a more appropriate response should be given.
- In column 6; natural risk is considered a risk because it equals risk appetite. However, these risks, like other risks, it needs to be monitored because of the possibility of change.
- In column 7, the response to risk has reduced residual risk below risk appetite. This indicates that an appropriate response has not been given, and therefore resources have not been used efficiently. In this case, it is necessary to determine the appropriate response that will equalize residual risk with risk appetite.

There are four main methods used in responding to risk, and these methods are shown in Figure 7.

Figure 7: Risk Response Methods



Acceptance: This is a response method that administrations find more appropriate. Risks may be acceptable in the following situations;

- Natural risk is acceptable if it falls within the realm of risk appetite.
- Measures are accepted if the benefits of taking them (controlling, delegating, or avoiding them) are found to be less than the cost of taking them.
- Some risks are beyond management control. Other risks do not disappear unless the activity is terminated, and terminating the activity is not always possible or desirable. In these cases, the risk is accepted.

Controlling: This is a method of responding to risk through control activities to keep risks at an acceptable level. This method is implemented through the control techniques listed below.

- Router Controls
- Preventive Controls
- Detection Controls
- Corrective Controls

* See the Control Activities section of the Guide for detailed explanation.

Delegation: This is a way of responding to risk by transferring activities that do not fall directly within the administration's core responsibilities, or that are deemed unsuitable for the administration to undertake due to cost-benefit considerations, and are therefore considered to carry high risks, to another administration/person/organization with the necessary expertise/equipment/resources. However, it should be remembered that even if the risk is delegated, the responsibility cannot be delegated. Because if the risk materializes, the administration itself will suffer the consequences. In this context, the delegation of risk should also be considered as risk sharing.

Examples of risk transfer:

- Delegating part or all of the activity to another administration with expertise in this area.
- Submitting the activity to third parties through a tender process.
- Transferring the risk using an insurance method (where applicable).

Avoidance: If the risk is too great to manage and/or the activity is not vital, it is possible to terminate the activity. For example, abandoning the construction of a factory that is expected to generate significant air pollution. However, in cases where public interest requires it, it may not always be possible for the administration to terminate activities. In such cases, alternative activities should be considered to provide the service or the activity should be postponed to a suitable period.

RY Box 15 outlines the process for responding to risks.

RY Box 15: How Do I Respond to Risks?

- **Prioritize risks and opportunities based on the analysis results.**
- **Determine your response based on the nature of the risk;**
Accept it
Check it
that Transfer
Run away!
- **Ensure that the benefit of the answer outweighs the cost.**

Evaluating Opportunities

When managing risks, the opportunities that risks create must also be taken into consideration. Alongside the negative consequences that risks bring, opportunities also occasionally arise.

In order to take advantage of these opportunities, which will provide additional contributions to the achievement of the administrations' goals, the administration needs to have predetermined strategies.

Seizing opportunities is not an alternative to responding to risks. It is a method that can be used with them.

However, taking advantage of opportunities should be evaluated within the framework of risk management and acceptable risk should be considered. In determining its level, both opportunity and cost-benefit analysis must be considered together.

Taking a slightly higher risk and/or a reasonable additional fee where the opportunity is deemed significant. Bearing the cost can be considered a managerial choice.

Opportunities may be available in the following situations:

- In situations where the reduction of threats and the realization of positive opportunities occur simultaneously. For example, conducting health and scientific research to find a cure for a disease (On the one hand, the threat of disease will decrease; on the other hand, there will be opportunities for lower costs as people go to hospitals less).
- In situations where opportunities arise before negative situations occur. For example, using new technology to work more effectively, or reaching more citizens through e-government.

RY Box 16 contains some tips that can be used in the process of responding to risks.

RY Box 16: Tips for Responding to Risk

- **Prioritizing risks helps in deciding which risk to respond to first.**
- **When determining the responses to risks as a public administration, those served (or indirectly) should be considered. (those affected) and the effects on them should also be considered.**
- **When responding to risks, it is necessary to avoid excessive control measures. Both a lack of control and excessive control harm the effectiveness of management.**
- **When responding to risks, it should be considered that coordinating with other administrations may be more effective.**

RY Box 17: Risk Response Methods - Example

Your administration has decided to purchase a new Information Technology (IT) system.

You identify your risks: Risk

1: Insufficient response time of the new system. **Risk 2:**

Failure to correctly transfer data from the old IT system to the new one. **Risk 3:** Lack of expertise to operate the new IT system.

Risk 4: The new IT system failing to work.

What kinds of responses can you give to these risks?

Risk 1:

Acceptance: You've been told the new IT system has a 5-second response time. Since this is similar to the current system, you might decide you don't need it to be faster.

Risk 2:

Verify: You need to define a verification activity to ensure the data is transferred correctly.

Routing controls: Sufficient IT personnel working on developing the new system.

You ensure that they possess the necessary qualifications and experience.

Preventive checks: You test the new IT system before accepting it to ensure that the data is not corrupted during transmission.

Detection checks: One month after the new system is put into operation, checks will be performed on the old system. You run tests to verify the accuracy of the continuous data transferred to the new system.

Corrective checks: If comparing the data transferred from the old system with the data in the new system reveals an error in data transfer, you will make/have the necessary changes made to the program.

Business continuity plan: You must ensure that you can reuse the old system if the new system fails to transfer data as needed.

Risk 3:

Transfer: You transfer responsibility for operating the new system to the service provider you purchased the service from for a reasonable period of time.

Risk 4:

Avoid: If the new IT system turns out not to work during testing, you would abandon the purchase. You would look for an alternative IT system.

Seize the opportunity: Your new IT system allows you to work more efficiently and leaves your staff more time to focus on other tasks.

7.4. Risk Review and Reporting

7.4.1. Risk Review

Risks can change in terms of impact and probability over time due to various changes in conditions or the measures taken. Furthermore, it is possible for new risk areas to emerge as conditions change. Therefore, all aspects of the identified risks and the risk management process should be reviewed periodically. Reviews should be conducted at least once a year, and at a frequency determined by the management based on the importance of the risks.



In the event of extraordinary developments that have a significant impact on predetermined risks, the IRK, upon verbal or written instruction from the senior executive, coordinates the immediate meeting of the IKIYK to assess the risks. Examples of extraordinary developments include natural disasters, economic crises, and the decision to hold early elections.

The review of risks and the risk management process are distinct processes; reviewing one does not mean the other has been reviewed. While risks are reviewed by each risk owner, the risk management process is reviewed by the senior management (or, if applicable, by the internal audit unit acting on behalf of the senior management) and/or the internal audit committee. Regularly reviewing risks and the risk management process will provide the management with flexibility in adapting to changing circumstances.

Risks are reviewed as follows:

- Whether risks still exist, whether new risks have emerged, and whether risks will materialize. It is reviewed whether there has been any change in their probabilities or effects.
- Priority in the review should be given to risks with high risk scores or key risks prioritized by management. However, the ideal scenario is to review all risks.
- When reviewing strategic risks, priority should be given to any changed policy documents, developments in other countries, public expectations for the period, internal audit reports, reports from inspection and audit (or guidance) units, external audit reports, and other relevant reports and documents.
- In light of developments, if a change has occurred in the risk profile, the administration/unit/subordinate The unit's risk record should be reviewed.
- Information about the change should be communicated to the next-level risk coordinator.
- Prioritization of key and/or significant risks at the strategic level should be reviewed, and the assessment results should be presented to the senior management by the IRK as a report following the IRK meeting.
- The conclusion and evaluation section of the report must include whether the risk management process provides sufficient assurance and whether new measures are needed. In this context, the following questions may be considered:

Do we provide reasonable assurance that the risks are managed successfully? That the responses to the risks are implemented or monitored effectively?

Are we providing reasonable assurances?

The risk review process, tips, and considerations can be found in RY Box 18 and...
This is summarized in section 19.

RY Box 18: Tips for Reviewing Risks

- **Determine a review period based on the nature of the activity. Review key risks frequently.**
- **During the review, assess the impact and probability of the risks for that period.**
- **Decide whether the risk is still above an acceptable level.**
- **Determine whether any new risks have emerged during that period.**
- **It is also necessary to review the status of responses to risks in light of changes in the risk situation.**
- **Record the findings in the risk log.**
- **Report the necessary risks (at every level).**
- **Changes related to risk are recorded in the risk log, but in very urgent cases, inform the next highest-level responsible person as soon as possible.**

RY Box 19: Questions to Consider When Reviewing Risks

- **Are there any changes in government and administration policy documents?**
- **What are the changes in environmental conditions?**
- **What internal changes affect the operation of the activity?**
- **What are the effects of the changes on management?**
- **Are the current controls sufficient to meet the changing situation?**
- **Is there sufficient evidence that the controls are effective?**

7.4.2. Reporting

Reporting is a crucial element in risk management that directly influences decision-making processes. It is of particular importance that reports are concise and brief, relevant, demonstrate evidence supporting assessments, and are submitted to the appropriate people at the appropriate time. Reporting within the administration should be done horizontally and vertically to the relevant individuals. The Risk Management Board (RSB) should clearly define who reports, to whom, and how frequently.

Reports shall be submitted to the administration using at least the information in the forms included in the appendix to this Guide. It must be done in formats determined by [the relevant authority] and at predetermined intervals.

Administrations may develop additional forms besides those included in the Guide if they deem it necessary.

8. LEARNING FROM EXPERIENCES

Risk management experiences by systematically using training tools
It needs to be enriched and presented to target audiences in the most effective way.

Depending on the target audience, methods such as conferences, seminars, workshops, training sessions, practical training, internships, information sharing through various communication channels, sharing best practices, and sharing negative examples or mistakes will facilitate the development of risk management processes and establish corporate risk management practices on a sound foundation.

Coping with risks largely depends on experience. Sharing past experiences, including both successful and unsuccessful approaches, through a strong communication network will facilitate more effective and faster responses to risks. In particular, sharing positive and negative experiences regarding newly

emerging risks and methods of dealing with them, and understanding what can go wrong, will prevent the repetition of mistakes and increase effectiveness in risk management.

Units at the same hierarchical level should learn from each other how they manage risks and improve. Applying these examples to themselves is a useful method.

Sharing experiences is a necessity in public administration in general. Because every These are not the resources of a single administration, but the common resources of the country. In this sense, sharing experiences is of particular importance in ensuring the effective use of resources.

In this context, treating experience sharing as a process and phasing it out (methods of identifying risks, monitoring the effectiveness of responses to risks, identifying failures, learning from them, sharing acquired experiences, etc.) will enable administrations to systematize experience sharing.

RISK MANAGEMENT APPENDICES

RY Appendix 1: Procedures to be Followed in Identifying, Assessing and Recording Risks Method**Step 1**

Bring together all members, representatives, or personnel working on the project or a specific work process of the unit or subunit in a suitable environment. Identify a suitable facilitator (see Box 20) to lead the brainstorming session. Brainstorming is most effective when led by someone experienced in facilitating such sessions.

(Note: Brainstorming can also be done by bringing together all senior executives in the administration to discuss strategic risks.)

Everyone participating in the brainstorming session should have sufficient knowledge of management and processes, in turn.

RY Box 20: The Facilitator's Role

- To ensure that all risk workshop participants actively participate in the risk identification activity.
- To explain the purpose of the program to the participants.
- To ensure that similar risks do not recur. (Combining very similar risks to suggest)
- To ensure all participants vote on the impact and probability of the identified risk.
- Encouraging participants to evaluate each other's scores, defend their own scores, or change their scores where they deem appropriate.
- Ensure that risk scores are accurately entered into RY Appendix 2: Risk Rating Form and To ensure prioritization.
- Developing an action plan to respond to risks, starting with the most urgent ones.
- Ensure that responsibility is assigned to a specific individual for each answer.
- Ensure that a specific review and reporting date is set for each response.

Step 2

First, clearly define the objectives of the unit/subunit/project/business process/administration. These objectives are defined in the strategic plan. However, they may not be defined for the subunits. Think broadly and discuss whether there are any other objectives that have been overlooked. All participants must agree on these objectives before proceeding to step 3.

Step 3

All participants in the brainstorming session should generate numerous ideas about the risks to achieving the goals identified in Step 2. This can be done as a single group or in subgroups for larger brainstorming sessions. Clearly identify which goal(s) might not be achieved if the risk materializes, and record the risks along with their associated goals in the Risk Rating Form (RRS Appendix 2, columns 3, 4, and 5).

Step 4

After all risks have been identified, brainstorming participants vote on the impact and probability of the risk. The votes are recorded on the Risk Voting Form. The number of relevant columns on the Form can be increased according to the number of participants (Columns 6, 7, 8 and 10, 11, 12). (When assigning impact and probability scores, please refer to Appendix 5. Sample Risk Assessment Criteria Table.)

Step 5

After the initial votes are recorded on the form, in cases where there is a significant difference between the highest and lowest scores given for the impact and/or probability of a particular risk, the person(s) who gave the highest score should first defend their reason for giving the highest score and try to persuade others to raise their own score. Then, the person(s) who gave the lowest score should defend their reason for giving the lowest score and try to persuade others to lower their own score. After the defenses are made, everyone who is convinced by any of the defenses should be given the opportunity to change their score.

Step 6

The risks identified in the Risk Voting Form are ranked from highest to lowest using risk scores (Column 14), which are calculated by multiplying the average impact (Column 9) and average probability (Column 13) from the brainstorming session. Participants are asked if the result met their expectations. Is the risk they consider most important the one with the highest score? If not, the voting results are reviewed again to determine if anything needs to be changed.

Step 7

After brainstorming participants agree on the risk scores in the Risk Rating Form, they transfer all risks, starting with the highest priority risk, along with their respective values, to the relevant columns of the Risk Record Form (RY Appendix 3).

Step 8

When determining the response to risks, consider whether the risk level is within the scope of risk appetite, which response would be most appropriate, and which would best mitigate the risks by reducing their impact and/or probability. Also, consider what the current risk responses are, whether they are currently effective and can be improved, and whether proposing new responses in addition to or in place of existing ones. Fill in the relevant columns in accordance with the explanations in the table (See Appendix 3: Risk Record Form - columns 6, 11, 12).

Step 9

The Risk Registration Form is completed by filling in the other columns (Columns 13 and 14), following the instructions on the form.

RY Box 21 contains some rules for brainstorming.

RY Box 21: Recommended Basic Rules for Brainstorming

- **Identifying a facilitator**
- **There is no such thing as a bad idea .**
- **Equal right to speak and limiting the time limit for speaking.**
- **Active participation**
- **Adherence to the timeline**
- **Guidance provided by the facilitator**
- **Open criticism, not personal criticism**

Risk Rating Form

It is used to identify risks and determine a risk score.

RISK VOTING FORM

1	2	3	4	5	6	7	8	9	10	11	12	13	14
				Identified Risk	Effect A	Effect B	Effect C	EFFECT	Possibility A	Possibility B	Possibility C	POSSIBILITY	Risk Score
				Risk									
				Reason				(A+B+C)/3				(A+B+C)/3	EFFECT X POSSIBILITY

Columns													
1	Sequence Number: Indicates the sequence number in the risk record.												
2	Reference Number: Indicates the reference number of the risk. The reference number is a coding system that also shows the unit to which the risk owner is affiliated. This code is not changed as long as the risk continues. The same code cannot be assigned to another risk.												
3	Strategic Objective: This column contains the code for the strategic objective to which the risk is associated, as defined in the strategic plan.												
4	Unit/Subunit Objective: If the risk record is filled out at the Unit/Subunit level, the objective that is directly or indirectly related to the administration's strategic objectives and will be affected by the risk is written in this column. If the risk record is filled out at the Administration level, this column can be left blank.												
5	Identified Risk: Risk: The identified risks are listed. Cause: The reasons that led to the occurrence of this risk are stated.												
6	7	8	Impact A/B/C: The name of each participant in the risk assessment studies and the score they gave to the impact are recorded in these columns. The number of these columns can be increased depending on the number of participants. Please refer to Appendix 5. Sample Risk Assessment Criteria Table when scoring.										
9			Impact: The arithmetic mean of the scores given by the participants is taken to find the (average) impact score of the risk.										
10	11	12	Probability A/B/C: The name of each participant in the risk assessment study and the score they gave to the probability are recorded in these columns. The number of these columns can be increased depending on the number of participants. When scoring, see: Appendix 5. Sample Risk Assessment Criteria.										



			Table
	13		Probability: The arithmetic mean of the scores given by the participants is taken to find the (average) probability score of the risk.
	14		Risk Score: The Risk Score is calculated by multiplying the Impact Score (average) by the Probability Score (average).

RY Appendix 3: Risk Registration Form

This form is used to record and report on risks identified at the administrative/unit/subunit level.

RISK REGISTRATION FORM

Administration/Unit/Subunit:													Date: .././20....	
------------------------------	--	--	--	--	--	--	--	--	--	--	--	--	-------------------	--

1	2	3	4	5	6	7	8	9	10	11	12	13	14
				Identified Risk	Responses to risk: Current controls					Responses to the risk: New / Added / Removed Controls		Risk Owner	Explanations
				Risk									
				Reason									

Columns	
1	Serial Number Indicates the ranking in the risk record.
2	Reference Number: Indicates the reference number of the risk. The reference number is a coding system that also shows the unit to which the risk owner is affiliated. This code is not changed as long as the risk continues. The same code cannot be assigned to another risk.
3	Strategic Objective: This column contains the code for the strategic objective to which the risk is associated, as defined in the strategic plan.
4	Unit/Subunit Objective: If the risk record is filled out at the unit/subunit level, the objective that is directly or indirectly related to the administration's strategic objectives and will be affected by the risk is written in this column. If the risk record is filled out at the administration level, this column is left blank.

5.	Identified Risk: Risk: The identified risks are listed. Cause: The reasons for the occurrence of this risk are stated.
6	Responses to the risk: Existing Controls: Existing controls are written in this column.
7	Impact: This is the impact value (between 1 and 10) determined using the Rating Form (see Appendix 2). Listing the control activities, measures taken, and regulations in place regarding the risk is helpful in this determination. It helps to identify the impact if the risk materializes despite existing measures.
8	Probability: This is the probability value (between 1 and 10) determined using the Voting Form (see Appendix 2). Listing the control activities, measures taken, and regulations in place regarding the risk is helpful in this determination. The probability of the risk occurring despite existing measures is determined.
9	Risk Score (R=ExO): Risk scores are calculated by multiplying the impact and probability values identified in the evaluation on the Voting Form (See Appendix 2), and are written according to predetermined high, medium, and low score ranges.
10	Change (Direction of Risk): This column shows the change in the risk status, taking into account the previous risk record. It can be indicated with text (up/down/fixed) or with directional symbols, depending on the administration's preference. If there is no previous risk record, it is indicated as "New".
11	Responses to Risk - New/Additional/Removed Controls: First, the necessity/adequacy of existing controls is assessed. If they are deemed adequate, no new controls are planned. If they are not adequate, new or additional controls are written. Controls deemed suitable for removal are also shown in this section.
12	Start Date: This is the exact date when any planned new or additional controls will be implemented, and any controls planned to be removed will be phased out. It is history.
13	Risk Owner: The person responsible for managing and monitoring the risk. The risk owner is the individual who collects information about the risk, conducts monitoring, manages responses to the risk, and maintains evidence that the risk has been managed. The risk owner must have the necessary resources and authority to implement responses to the risk. The risk owner is also responsible for updating risk records and reporting to a higher authority regarding the risk.
14	Explanations: This column describes the current state of the risk, the direction of change, when it will be reviewed, the reporting intervals and to whom it will be reported, and any other details that need to be specified.

Colors	
	High level of risk
	Moderate risk
	Low risk

NOTE: If a new risk is identified during the year, the employee who identified the risk will report it to a senior manager. If the manager decides that it is a risk that needs to be managed, the risk will be recorded in the Risk Record Form and approved by the relevant manager.

RY APPENDIX 4: Consolidated Risk Report

It is used to report risks identified at the administrative/unit/subunit level to a higher level of management.

CONSOLIDATED RISK REPORT

Administration/Unit/Subunit:					Date: .../.../20....			
1	2	3	4	5	6	7	8	9
				Identified Risk	Situation		Risk Owner	Explanation
					Previous Risk Score and Color	Current Risk Score and Color		

Columns	
1	Sequence Number: Indicates the sequence number in the risk record.
2	Reference Number: Indicates the reference number of the risk. The reference number is a coding system that also shows the unit to which the risk owner is affiliated. This code is not changed as long as the risk continues. The same code cannot be assigned to another risk.
3	Strategic Objective: This column contains the code for the strategic objective to which the risk is associated, as defined in the strategic plan.
4	Unit/Subunit Objective: If the report is prepared at the unit/subunit level, the unit/subunit objectives listed in the Risk Record Form are entered in this column. If the report is prepared at the administrative level, this column is left blank.
5	Identified Risk: The identified risk is written here.



6	Previous Risk Score and Color: Indicates the status of the risk in the previous Consolidated Risk Report.
7	Current Risk Score and Color: Indicates the status as of the report date.
8	Risk Owner: The person responsible for managing and monitoring the risk. The risk owner is the one who collects information about the risk, performs monitoring, manages responses to the risk, and maintains evidence that the risk has been managed. The risk owner must have the necessary resources and authority to implement responses to the risk. The risk owner is also responsible for updating risk records and reporting to a higher authority regarding the risk.
9	Explanation: The effectiveness of the control activities and future projections are included in the explanation section.
Colors	
	High level of risk
	Moderate risk
	Low risk

RY Appendix 5: Sample Risk Assessment Criteria Table

		Possibility	Effect			
			Strategy	Activities/processes are	Financial	Compliance with Legislation
10	High	...these are the risks that are almost certain to occur in achieving strategic goals within a year/month/day. These are the risks that the administration may have an impact on. When the structure is	of significant material and economic impact on the activities of the Administration/unit/sub-Administration/unit/sub-unit. Risks that can lead to loss in an efficient way; inability to achieve it. The risks that public resources will face, and which are acceptable to the administration, fall into this category at this level.	of significant material and economic impact on the activities of the Administration/unit/sub-Administration/unit/sub-unit. Risks that can lead to loss in an efficient way; inability to achieve it. The risks that public resources will face, and which are acceptable to the administration, fall into this category at this level.	Risks that can lead to loss in an efficient way; inability to achieve it. The risks that public resources will face, and which are acceptable to the administration, fall into this category at this level.	These are the risks involved in situations where failure to comply with regulations, whether intentional or unintentional, can create significant liabilities for the administration/unit/subunit.
9		considered, the probability of the administration deviating from its policy or procedures, and therefore the wider the scope of activity, is the greater the likelihood of events occurring, and the greater the probability of the administration failing to adequately achieve its objectives.				
8						
7		It is that high.				
6	Middle	These are risks that are likely to occur within a year/month/day. These are generally risks that the administration/unit/subunit has previously faced, or risks that have been encountered in general. administrations in	specific unit/subunit in achieving strategic goals and range, cannot potentially be effectively and economically utilized to achieve key strategic goals at a level acceptable to the administration.	The risks that could cause financial loss for, economical, and potentially impactful. These are risks that, while falling within this score	to-medium risk should	These are risks that may create certain levels of liability for the administration/unit/subunit if compliance with the legislation is not ensured, whether intentionally or unintentionally.
5						
4						
3	Low	These are things that are unlikely to happen within the year/month/day. These are risks.	It may have little impact on achieving strategic goals.	The risks involved are those that will cause minimal financial loss for the administration/unit/sub-administration/unit/department service		Failure to comply with regulations, whether intentionally or unintentionally.

Kamu İç Kontrol Rehberi		 Risk Yönetimi				
2		These are generally risks that the administration/ unit/subunit encounters very rarely, and whose probability of occurring is almost nil.	These are risks. The effects are generally minor and cover a limited area.	These are risks that may have little effect on whether it can be carried out effectively, economically, and efficiently.	The misuse of public resources by the administration, or spending below a certain amount, is considered low risk.	These are the risks in situations where very low levels of obligations and/or responsibilities may arise on the administration/unit/subunit.
1						

EXPLANATION: The information in the table regulates the general principles for assigning impact and probability scores to risks. Both risk categories (strategy, activities/processes, financial, regulatory compliance, etc.) and risk criteria should be determined by the administrations themselves, specific to their respective areas of responsibility.

RY Appendix 6: Case Study on Natural and Residual Risk

A case study to highlight the concepts of natural and residual risk, and to demonstrate how a risk owner can obtain information from various control officers (individuals responsible for the relevant risk within the framework of division of labor) to monitor the extent to which the risk for which they are responsible has been successfully mitigated through existing controls.

This case study involves a warehouse containing gold bars, the warehouse manager who faces the risk, the risk of theft of the gold bars, and four control activities:

Control 1: The Information Technology (IT) system monitors the gold bars entering and leaving the warehouse; a record of the gold bars entering and leaving the warehouse is kept every business day, and the IT manager reports this record to the risk owner daily.

Control 2: An independent company visits monthly to count the gold bars in the warehouse and reconcile them with the IT manager's report. (Any discrepancies between the report and the stock are investigated and explained if possible.) The independent company sends a monthly report to the risk owner detailing any unexplained discrepancies (unexplained discrepancies could include potential theft cases).

Control 3: Security Guards - Professional security guards control access to the warehouse 24/7, ensuring only authorized personnel enter and all bags pass through a metal detector upon leaving the building, thus preventing the smuggling of gold bars (the bars are too heavy to easily conceal/carry). During recruitment, security guards' criminal records are checked (gold bars are too heavy to easily conceal/carry). Security guards report to the risk owner once a week.

Check 4: Alarm system - alarm activation incidents are reported to the risk owner. Security personnel regularly (weekly) check the operation of the alarm system, and the results of the check are included in the report sent to the risk owner.

In the absence of the four controls listed above, the inherent risk is considered high risk. This would be above risk appetite, and consequently, the four controls listed above are designed to reduce the risk of theft of the gold nuggets, and the anticipated effect of these four controls is the reduction of residual risk (Note: these four control activities will only reduce the probability of theft of the gold nuggets, not its effect).

The risk owner will gather evidence regarding the effectiveness of these four controls. If the controls are found to be effective, the risk owner will examine whether the risk has been successfully reduced within acceptable risk limits.

If the risk owner finds one or more of the above controls to be ineffective, the risk will likely remain above the acceptable level, and thus the risk owner will need to communicate this problem to their manager and propose methods to mitigate the risk (either by introducing additional controls or strengthening the ineffective controls).

CHAPTER THREE

CONTROL ACTIVITIES

1. INTRODUCTION

Control activities aim to reduce the impact and/or probability of a foreseen risk, thereby enabling management. These are actions aimed at increasing the likelihood of achieving one's aims and objectives.

Determining control activities depends on the completion of the risk assessment.

Management should plan, organize, and direct control activities based on risk management to obtain reasonable assurance that tasks and objectives will be achieved.

Control activities encompass financial and non-financial controls and cover all activities of the administration. It should be designed and implemented as a whole.

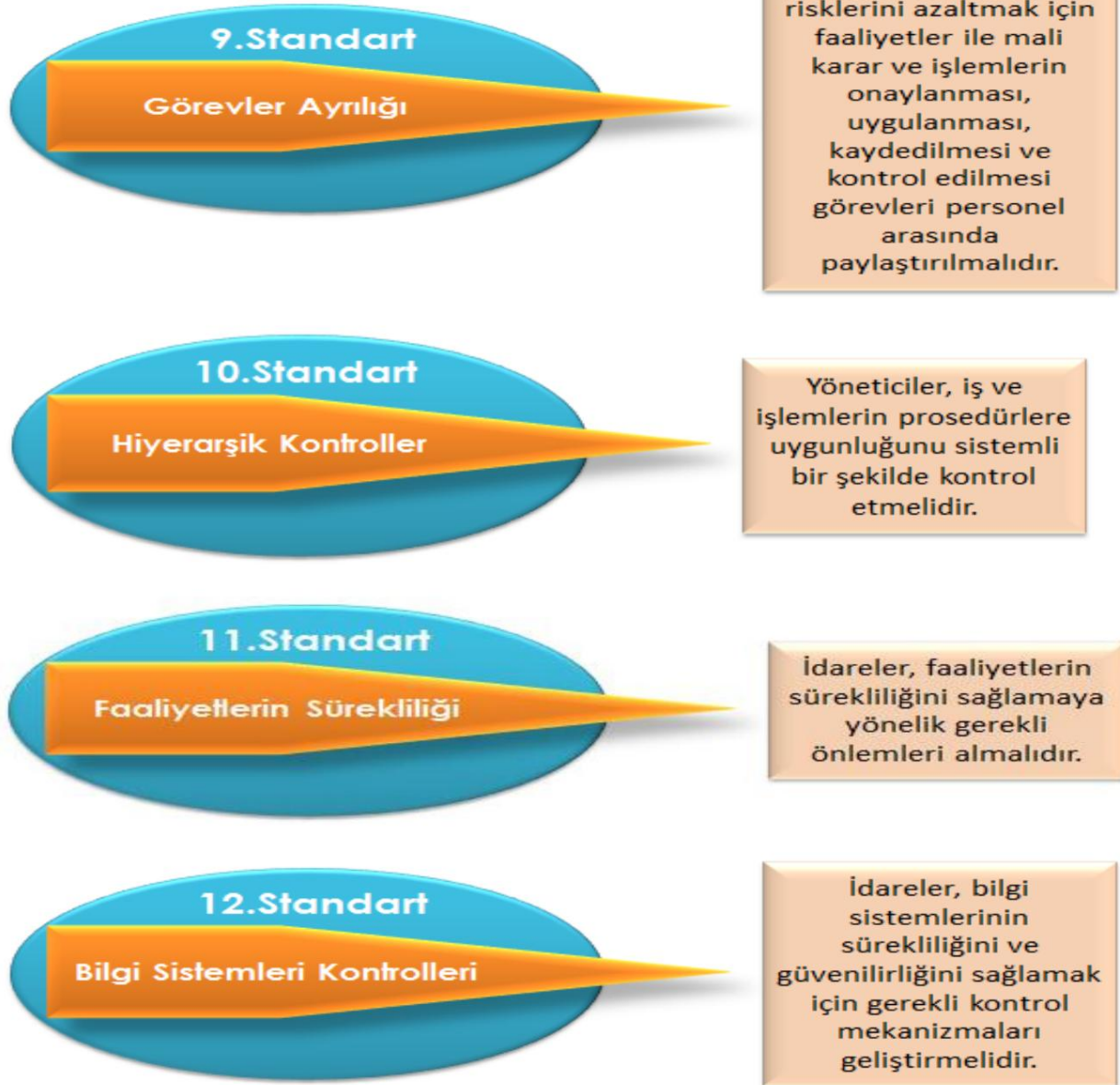
This section of the guide provides users with information on control activity procedures to ensure the effective management of risks to the administration's achievement of its objectives, within the framework of the Public Internal Control Standards listed below.

2. CONTROL ACTIVITY STANDARDS

Administrations shall use the standards contained in KF Box 1 and these when defining and implementing control activities. They take into account the general requirements regarding standards.

KF Box 1: Standards for Inspection Activities





3. CONTROL ACTIVITIES PLANNING PROCESS

Control activities involve assessing the risks that administrations foresee while carrying out their decisions, activities, and procedures. They are tools developed to overcome challenges.

Within the framework of cost-benefit analysis of control activities, directly achieving the objective. It needs to be designed in a way that will provide this.

Ideally, risk management processes and control activities should be incorporated into systems and processes when those systems and processes are being created. This is because implementing control activities at a later stage may be more costly and less effective.

Ensuring that control activities are understandable, implementable, and consistent is crucial for control effectiveness. A good control strategy should consider not only the identification of controls but also how they will be implemented, taking organizational capacity into account.

Another key consideration in planning control activities is the implementation of... It is the process of evaluating the effectiveness of controls.

It is necessary to evaluate whether the intended outcome aligns with the purpose of the control measure, and whether there is a correlation between initial costs and actual costs.

Furthermore, regularly reviewing control activities in light of changing circumstances is also an important aspect of evaluating their effectiveness.

Administrations should consider the basic requirements in KF Box 2 when determining control activities.
should receive:

KF Box 2: Essential Requirements

Control activities must:

Be adequate (the right control is in the right place and at the right level),

- **The cost of implementing the control should not exceed the expected benefit,**
- **It should be comprehensive, understandable, and directly related to the risk.**
- **It must be documented,**
- **By evaluating it as a whole and ensuring its consistency,**
- **Continuing until its effectiveness is evaluated,**

is necessary.

4. CLASSIFICATION OF CONTROL ACTIVITIES

Control activities are generally classified as directive, preventive, detection, and corrective controls. However, depending on the nature of the risk, it is possible for administrations to implement additional control activities if deemed necessary.

For examples of control activities, see KF Appendix 1: List of Sample Control Activities.

4.1. Router Controls

It is a method of controlling risks through indirect activities such as informing, protecting, and setting courses of action.

KF Box 3: Examples of Router Controls

- An accepted organizational chart that is continuously updated to reflect organizational changes
- Practical materials such as guides, official statements, handbooks, brochures, and posters
- Written unit and sub-unit job descriptions regarding aims, objectives, activities, and projects.
- Prepared in accordance with job descriptions, taking into account the titles, knowledge, and experience of the individuals.
- task assignment charts
- Written delegations of authority in accordance with legislation, hierarchical structure, and the requirements of the job are necessary for the effective performance of tasks.
- Effective communication and reporting tools within the organization

4.2. Preventive Controls

To reduce the probability of risks occurring and keep them at a level acceptable to the administration. These are the checks that need to be done.

KF Box 4: Examples of Preventive Controls

- Security of tangible and intangible rights (intellectual property, etc.) and records
- Physical preservation of assets
- Recording of financial and administrative information • Establishing access controls such as passwords, identity cards, and security personnel • Implementing the principle of separation of duties to prevent conflicts of interest
- Preliminary financial control procedures

4.3. Detection Controls

These are inspections carried out to determine the extent of damage and losses that occur after risks have materialized.

Detection checks are primarily carried out to determine whether risks have materialized. These checks also have a mitigating effect on the likelihood of risks occurring. Inspections carried out to determine the extent of damage and losses after risks have materialized are also included in this scope. Post-expenditure inspections should also be considered within this context.

KF Box 5: Examples of Detection Controls

- Periodic counts/physical inventories • Comparison of counts/inventories with records • Determining appropriate methods for identifying and analyzing discrepancies

4.4. Corrective Controls

These are controls aimed at mitigating the effects of undesirable consequences in situations where risks materialize.

KF Box 6: Examples of Corrective Controls

- Identifying methods to compensate for losses and damages that may negatively impact operations.
- Implementing the necessary measures to correct and eliminate the identified discrepancies.
- Including a provision in contracts for the recovery of undue payments
- Estimation of the warranty period

5. CONTROL ACTIVITY METHODS

While the main control methods are listed below, administrations may also apply different pre-implementation (ex-ante) and post-implementation (ex-post) control methods as needed, according to their areas of responsibility and organizational structures.

Pre-implementation checks are carried out by following appropriate procedures before the activity is performed . These are the controls that have been put into practice.

Post-implementation controls are carried out by management after the organization's activities have been completed. It means being subjected to control by predetermined methods.

KF Box 7: Tips for Control Activities

- Reducing both the probability and impact of internal risks through control activities. It is possible.
- Reducing the probability of external risks materializing may not be within the control of the administration. However, the risks... Mitigating its effects will be possible with proper risk management.
- When identifying control activities and allocating resources to these activities, prioritization based on risk score is taken into account. However, according to the Risk Map, it may be necessary to prioritize risks with a high probability but low impact (See RY Figure 4: Risk Map).
- For risks with a very high probability and impact, business continuity is implemented in addition to control activities. It is also very important to prepare plans.
- When responding to risks, it is necessary to avoid excessive control activities. Both a lack of control and an excessive amount of control harm the effectiveness of risk management.
- Depending on the nature of the risk, several control methods may be used together if necessary.
- Cost and benefit analyses of control activities should be conducted. • Pilot applications of control activities can be carried out when necessary to see if they are creating the desired effect.
 - The effectiveness and operation of control activities should be monitored to ensure they are implemented as planned. Necessary evidence regarding the effectiveness of controls should be collected and analyzed periodically.
- After a reasonable period, the effectiveness of new control activities and ongoing existing controls should be evaluated and reported to the manager/risk coordinator.

When determining control activities, the points in KF Box 8 should be taken into consideration.

KF Box 8: Factors to Consider When Determining Control Activities

Control activities;

- Who(s)/which unit(s) will carry it out?
- Targeted completion dates
- Resources required for implementation
- Critical success factors
- How to document it
- Processes for monitoring

It must be determined in advance.

5.1. Decision Making and Approval

Decision-making and approval authorities in activities must be clearly and in writing defined. Decision-making and approval should only be done by authorized persons. The authorization procedure should cover specific conditions and the delegation of authority by managers to employees in particular activities.

Compliance with the authorization order means that employees act in accordance with instructions and the organization's or They must operate within the limits set by the legislation.

5.2. Separation of Duties

Managers should establish rules that assign responsibility to different employees at different stages of a transaction, process, or activity—such as approving, implementing, recording, and controlling—in situations where the risk of error, irregularity, corruption, and breaches is high.

Implementing this distinction is more difficult in administrations with a small number of personnel. In such cases, management may consider combining two of these stages and compensate for the operation of this control mechanism with other mechanisms such as employee rotation, task rotation, or additional management controls.

This reduces the risk of a single person being involved in multiple aspects of a risky process or activity for an extended period.

5.3. Double Signature Method

The double signature method is applied to ensure the accuracy of the data in the document.

The double signature method is used in non-financial processes such as information submitted to senior management (reports, memos, statistics, etc.) and appointment orders, as well as in financial obligations such as payments (payment orders, etc.). It can be implemented before it happens.

Thus, especially in financial transactions, the accounting officer is informed of liabilities or payments, ensuring that accounting transactions are carried out correctly. The double signature method guarantees that the activities are performed by authorized persons.

The double signature method is a procedure designed to ensure the accuracy of the data in a document.

The double signature method involves sharing responsibility for certain information and evidence produced by the administration. It signifies undertaking.

Practices such as board decisions, tender committee decisions, and minutes, where authority and responsibility are shared simultaneously, can be included in this scope. Administrations can use similar practices in different areas according to their needs.

5.4. Data Reconciliation



To ensure consistency, data from different documents and sources should be compared. Matching must be ensured.

For example, reconciling account entries related to bank accounts with correspondent bank statements; matching invoice information with information on the movable asset transaction slip, etc.

5.5. Monitoring Procedures

The procedures for assigning and fulfilling tasks are determined by the managers. It should be monitored periodically.

Managers delegate tasks to others while simultaneously overseeing the execution of those tasks. It does not absolve them of their responsibilities.

Managers ensure that tasks are correctly understood and that irregularities and errors are prevented. The supervisor should give the necessary instructions to the staff and provide the necessary guidance and control.

Managers should also apply these procedures to ensure that the assigned task is completed correctly.

5.6. Preliminary Financial Control

Preliminary financial control is the control exercised over the financial decisions and transactions of administrations regarding their revenues, expenditures, assets, and liabilities; ensuring their compliance with the administration's budget, budget allocation, available appropriation amount, expenditure program, financing program, central government budget law, and other financial legislation; and ensuring the effective, economical, and efficient use of resources in expenditure units.

The purpose of pre-financial control is to ensure that managers' decisions/measures and financial activities comply with legislation and budgets, and that resources are used effectively (See: Procedures and Principles Regarding Internal Control and Pre-Financial Control).

5.7. Procedures Related to Accounting Operations

These procedures include accounting records of all financial transactions up to a specific date, in accordance with the relevant legislation. It must be ensured that it is done in accordance with the specified principles and rules.

The purpose of these procedures is to support the making of sound decisions on matters that may have financial consequences. (See: General Administrative Accounting Regulation, Central Administrative Accounting Regulation)

5.8. Anti-Corruption Procedures

Governments should announce written rules and procedures for reporting, investigating, identifying, and documenting administrative weaknesses, inconsistencies, and violations that lead to corruption and irregularities.

Anti-corruption procedures should include the following:

- Preventive controls; •

Procedures for identifying and reporting early signs of corruption and irregularities; • Whistleblowing procedures (See Information Communication Section); • Procedures for reporting irregular activities to external authorities such as the Public Prosecutor's Office. procedures.

5.9. Access to Assets and Information

Administrators must ensure that only those responsible for the protection and/or use of assets and information are authorized to access them.

Restricting access to assets reduces the risk of their misuse or improper use, and protects the organization from losses.

The level of restriction depends on the sensitivity of the assets and information, and the risk of misuse or loss. When determining the sensitivity of assets, managers should consider their value, portability, and convertibility to cash.



5.10. Documentation, Archiving, and Storage of Information

To support sound decision-making and process control within the administration, documentation, archiving, and information storage procedures should be established.

Documentation involves recording decisions made, events and actions that occur, and transactions carried out. The goal is to create written evidence. Documentation must be complete, accurate, and timely.

Documentation procedures should ensure that every document, action, and process within the organization is tracked by specifying who did what, how, and when, and the type and purpose of the resulting document/information. This is achieved through the creation of **an audit trail**.

Creation of an audit permit;

- Ensuring transparency, • Monitoring processes within the institution from start to finish,
- Approval, implementation, recording, and control of activities or processes such as following the stages,

It helps.**The audit trail reveals**

what procedures or processes are in place, who is responsible, what documents are prepared, and what management and control systems are in place for information flow.

It should specify which methods were used and how the results are presented.

Archiving procedures involve

organizing documents relating to past events, decisions, and actions of the institution in a chronological and systematic manner. They must ensure that it is filed. Procedures should be established to define the creation, completion, use, and destruction of archives.

Information**storage procedures**

must ensure that the information medium (paper and/or electronic) and the content of the information are stored without alteration to accurately reflect decisions and actions.

5.11. Business Continuity Plans

To ensure the continuity of service in the face of the risk of disruption to daily operations, necessary measures have been taken. It must be available.

Furthermore, there is a possibility of disruption to vital operations that could affect the administration's aims and objectives. Business **continuity plans** are necessary.

5.12. Information Technology Control Activities

Information technology (IT) requires specific control to be determined by managers in administrations. It requires mechanisms.

These mechanisms for controlling information systems include **general controls** and **application controls**. They are divided into two groups.

General control mechanisms are those that can be applied to all processes and contribute to their proper execution.

Implementation control mechanisms, on the other hand, encompass both the procedures programmed within the software product itself and the procedures that must be implemented by relevant personnel to control the operation of different processes.

Application control mechanisms require general control mechanisms to function.

The inadequacy of general controls cannot be compensated for by implementation controls.

Generally, general control mechanisms are used in data analysis and processing centers to define the installation, repair, and access to information of industrial software products: • **Data analysis and**

processing center control: These controls include defining the duties and responsibilities of the relevant data manager/operator, procedures for recording and subsequent use of information, computer backups, and emergency action plans.

• **Software controls:** These controls encompass the acquisition, installation, and continuous use of software products necessary for ensuring the overall continuity of the information technology system and the operation of software applications.

• **Access controls:** These controls provide protection against unauthorized access. In this context, they limit user access rights by allowing users to perform actions only with specific software products, thus ensuring separation of responsibilities.

General software controls created during system development require detailed application testing to verify the program's suitability and ensure all errors are detected.

Once the system is established, controls on access to and maintenance of the system ensure that no one can use or modify the applications without proper authorization, and that all necessary changes are made in accordance with the specified authorization and approval procedures.

Application control mechanisms prevent the entry of incorrect data into the system, correct errors based on automated procedures that verify the data form and its content, and thus support internal control.

Application control mechanisms analyze data simultaneously with its input into the system, identifying errors. If errors are detected, they are continuously reported and these errors are corrected immediately.

Implementing both types of control ensures that the information is analyzed and processed completely and accurately.

5.13. Evaluation of the Benefits and Costs of Control Activities

Risk is assessed after identifying control activities to reduce its impact and probability. Those responsible should evaluate the cost and expected benefits of the control activity.

If the cost of a control activity outweighs the expected benefit, that control activity should be avoided.

Benefit-cost analysis is an ongoing control activity and must be conducted in writing and approved by the appropriate level of authority for control activities that require a certain monetary value. (See Appendix 2 of the Benefit-Cost Analysis for examples)

6. IMPLEMENTATION STAGES OF CONTROL ACTIVITIES

The implementation stages related to the control activities are summarized in Table 1 of the Turkish Data Protection Regulation (KF).

Because control activities are linked to risks, stages 1, 2, and 3 deal with risk management, while stages 4 and 5 deal with control activities. For detailed information on stages 1, 2, and 3, please refer to the Risk Management section.

Table 1: Stages of Control Activity

Stage 1 ÷ Stage 2	Stage 3 ÷ Stage 4	Step 5
Setting goals	Identifying and assessing the risks in achieving the objectives. Responding to risks giving Determining the method: • Acceptance • Checking • Transfer • Avoidance Taking advantage of opportunities*	Classification of control activities: • Router • Preventive • Detector • Corrective
		Identifying control activities: • Decision-making and approval • Separation of duties • Double signature method • Data reconciliation • Monitoring procedures • Preliminary financial control • Procedures related to accounting transactions • Anti-corruption procedures • Access to assets and information

				• Documentation of information, archiving and storage • Business continuity plans • Information technology control activities Or: See KF Appendix 1: Sample Control Activities List.
--	--	--	--	--

* Seizing opportunities is not a response to risks, but rather a matter to be considered at every stage.

7. STEPS TO BE FOLLOWED WHEN DETERMINING AND IMPLEMENTING CONTROL ACTIVITIES

Step 1: When assessing risks, systems and processes are examined to determine if existing controls related to the risks exist. (Considering that risks are being assessed for the first time within the framework of the principles in this Guide, it would be beneficial for administrations to create an inventory of all their existing controls and review them, thus eliminating controls that cannot be matched to the administration's objectives and a specific risk.)

Step 2: Evaluate whether existing controls are effective/adequate in controlling the risks.

Step 3: If no existing control is found or if it is determined that it is ineffective/inadequate, a new and/or additional control activity is identified (Appendix 1, Sample Control Activities List, can be used as an aid in identifying the control activity).

At this step, it will be helpful to consider the following: • It may be appropriate to select

more than one control activity. • A cost-benefit analysis

should be performed for any new control activity you choose. • Suitable control activities should be tested beforehand.

Step 4: Risks that are assessed as being managed effectively/adequately through existing control activities. No new control activities are foreseen in this regard, and existing controls will continue.

Step 5: After the risk record is approved by the risk managers, new control activities are implemented on the foreseen start date, and the risk managers are required to ensure that both the new controls and the existing ongoing controls are monitored.

Step 6: Internal and external stakeholders regarding common risk areas are informed in writing about the relevant control activities and whether they are being effectively implemented.

Step 7: When reporting risks, the risk owner informs the manager/risk coordinator in the "Description" section of the Consolidated Risk Report (CSR Appendix 4) how the new control activities and ongoing existing controls are performing. This reporting is done by summarizing what happened, specifying the effects of the new control activities and ongoing existing controls, and attaching any evidence to the report.

CONTROL ACTIVITIES APPENDICES

KF Appendix 1: Sample Control Activity List

Category	Control Activity
Risk management	
The organization has appropriate risk management policies, procedures, techniques, and mechanisms for each of its activities.	Management has ensured the identification of risks related to objectives and activities by fulfilling the risk identification and assessment function. • By assessing the risks, management has determined the necessary actions and control activities and directed their implementation.
Implementation of control activities	
Control activities have been defined and are being implemented as required.	Management has accomplished the following: • Managers and employees have understood the purpose of the control activities. He/She is aware; - Control activities are carried out in accordance with the strategy determined by RSB; - Assigned personnel review the functioning of designated control activities and are prepared for situations where excessive controls need to be reduced to an appropriate level. - Regarding current control activities, the following are examined to determine their absence: 1. Guidance: Providing instructional information showing how the work should be done. Documentation: New documents There should be standard document control procedures that ensure the recording, 2. filing, recording of changes to documents, and archiving of files. 3. Control: This involves the manager checking the work done by personnel, including basic control activities such as cross-checking (where personnel in one department check the work of personnel in another department) or computer-based checks. 4. Security: Protection of documents, cash, and assets. 5. Emergency arrangements: Ensuring the continuity of essential services when unexpected situations arise.
Performance monitoring	
Senior management monitors the results of the performance program.	- Senior management participates in preparing an annual performance program, setting goals, and measuring and reporting results related to these programs and goals. - Senior management budget, forecasts and previous period budget - If, as a result of monitoring and evaluation, it is determined that the actual performance is lower than the target, senior management takes the necessary measures.
Managers monitor performance in light of objectives.	- All managers review activity reports and, in light of the objectives It measures the results. - Managers review financial performance, budget performance, and operational performance and compare them to planned results.

Category	The control activity
	compares. The analysis and examination of performance indicators and results are used for both operational control and financial reporting control purposes.
Quality of performance measurements and indicators	
Managers monitor the quality of performance metrics and indicators.	- Managers review and validate the appropriateness and accuracy of performance metrics and indicators at regular intervals. - Performance indicators are evaluated to determine whether they are related to and consistent with the mission, goals, and objectives. - Actual performance data is periodically compared against planned objectives, and differences are analyzed to see if the right things are being measured at the right time.
Human resources management	
The organization effectively manages its workforce to achieve its aims and objectives.	- The organization's mission and vision, goals, values, and strategies are outlined in the strategic plan, annual performance program, and other documents, and employees are informed about them. - The organization has a human resources planning strategy that includes workforce planning policies, programs, and practices aligned with the strategic plan and performance program. Senior management supports teamwork, strengthens the organization's shared vision, and encourages all employees to provide feedback. - Senior management adopts and encourages the implementation of a performance management system aligned with the organization's vision and mission. - The organization has a recruitment plan and procedures in place to ensure the recruitment of appropriately qualified personnel according to its identified needs. - Employees are provided with the information, training, and tools to enable them to fulfill their duties and responsibilities, improve their performance, develop their skills, and meet the changing needs of the organization. - Performance evaluations are conducted and feedback is provided to help employees understand the connection between their performance and the achievement of organizational goals.
Information processing	
The organization implements various control activities that comply with its information processing systems to ensure that the information is accurate and complete.	- Software checks are implemented to verify data entry. - Transactions are accounted for in numerical order. - File totals are compared with control accounts. - Exceptions and violations arising from other control activities are examined and acted upon as necessary. - Access to data, files, and programs is appropriately controlled.

Category	Control Activity
Physical Inspection of Sensitive Assets	
The institution implements physical controls to secure and protect its sensitive assets.	- Physical protection policies and procedures are developed and implemented, and This is announced to the staff. - Regularly tested, updated and provided to personnel A disaster plan is developed and announced. - Assets that are particularly vulnerable to loss, theft, damage, or unauthorized use, such as cash, securities, movable and immovable property, and equipment, are physically protected, and access to them is controlled. - Assets such as cash, securities, movable and immovable property and equipment are periodically inventoried and compared with control records, and discrepancies are also investigated. • The physical security of valuable documents is ensured and Access to these is subject to strict control. - Electronic signature machines and seals are physically protected, and access to them is strictly controlled. • Identification cards and numbers are attached to movable property or equipment. • Buildings are equipped with fire alarm and water spraying systems. - It is protected from fire. - Buildings are also monitored outside of working hours. (alarm, camera) etc.)
Separation of Duties	
To reduce the risk of errors, waste, and irregularities, high-risk and sensitive tasks and responsibilities are distributed among different individuals.	- No single person should be given the authority to control all the risky aspects of a transaction or activity. - The tasks and responsibilities required for significant transactions and activities in terms of authorization, approval, registration, payment, collection, review, auditing, protection, and management of related assets are carried out by different individuals.
Authorization regarding transactions and activities	
Appropriate personnel are authorized to handle operations and other essential activities.	- Transactions and activities are initiated and carried out in accordance with management decisions and instructions. - All processes and activities are carried out only by employees acting within their authorized scope. • Authorizations, including the specific terms and conditions to which the authorization is subject, are communicated to managers and employees. • Authorizations comply with legislation and internal regulations. - It is appropriate and within the specified limits.
Recording of transactions and activities:	
Transactions and significant activities are appropriately classified and recorded.	To help management make sound decisions and control operations, processes and activities are properly classified and recorded.

Category	Control Activity
Accountability for resources and records, and restricted access to them.	
Access to resources and related records is restricted, and it is clearly defined who will be responsible for them.	• The risk of unauthorized use and loss of resources and records is controlled by ensuring that only authorized personnel have access to them. • Resources and their related records are regularly compared, and inconsistencies are investigated. • The frequency with which resources are compared with records and the degree of access restrictions are determined based on factors such as the level of risk in protecting the resources, the value of the assets, their portability, and their convertibility into cash.
Certification	
The transaction is documented in accordance with activities and regulations.	• Documents are kept readily available for use and inspection at all times. All documents and records are properly managed, maintained, and updated at regular intervals.
General computer controls	
The institution regularly reviews its information systems. It conducts a comprehensive, high-level assessment of the risks it faces.	• Risk assessments are carried out and documented whenever systems, facilities, and conditions change, and at regular intervals. • Risk assessment takes into account data sensitivity and consistency.
Effective computer security controls are in place and being monitored.	• A plan has been developed that clearly defines the organization-wide security program, along with supporting policies and procedures. • Senior management has established a structure for implementing and managing the organization-wide IT security program, and related responsibilities have been clearly defined. • The organization monitors the effectiveness of its security plan and makes changes to the plan as needed. • Corrective actions are implemented promptly and effectively. It is tested and monitored regularly.
Effective computer access controls are in place and being monitored.	• Information resources are classified according to their importance and sensitivity. • The method and relevant criteria for resource classification have been determined and communicated to resource managers. • Resource managers have classified their own information resources according to the determined criteria and risk assessments, and have documented these classifications. • Resource managers have identified authorized users, and these individuals have been officially granted access to the information. • The institution monitors access to information systems, investigates obvious violations, takes appropriate corrective actions, and implements necessary measures. • To prevent or detect unauthorized access within the institution... Physical and logistical controls are in place.
Application software development and modification controls are in place and monitored.	• Application software changes are properly authorized. • All new or modified software is thoroughly reviewed. Tested and approved. • All key activities are monitored.

Category	Control Activity
Effective system software controls are in place and being monitored.	- Access to system software is restricted and access permission is documented based on job responsibilities. - Access to and use of system software is controlled and It is monitored. - Changes made to the system software are checked.
An effective separation of duties exists for IT operations.	- Conflicting tasks have been identified, and policies have been implemented to differentiate between them. - Access controls have been adopted to enforce task separation.
Controls ensure the continuity of IT services.	- The importance and sensitivity of computer-based operations have been assessed and prioritized, and support resources have been identified. - Measures have been taken to prevent and minimize potential damage and disruption through data and program security procedures, including backup data storage, environmental controls, personnel training, and hardware maintenance and management. - Management has developed and documented a comprehensive emergency plan for the IT service. - The emergency plan is tested at regular intervals, and actions deemed appropriate are taken. - Necessary changes will be made in those places.
Computer application controls	
Source documents are checked and require permission.	- Access to source documents is restricted. - Source documents are pre-numbered sequentially. - Access to key source documents requires an authorization signature. - Dataset control charts are provided in dataset application systems, containing information such as date, control count, document count, and checksums in key fields. - Before entering the application system, data is either at a high level or - It is reviewed independently. - Access to data entry terminals is restricted. - Master files and exception reporting are used to ensure authorization of all processed data.
Completion checks	- All authorized operations are entered into the computer and on the computer is processed. - Data reconciliation verifies that the data is complete.
Accuracy checks	- Data entry is designed to support the accuracy of the data. - Data validation and spelling to identify erroneous data. - Correction procedures are carried out. - Erroneous data is found, reported, investigated, and processed quickly. It will be corrected. - Output reports are reviewed to maintain the accuracy and validity of the data.
Integrity check of transaction and data files	Procedures ensure that the latest available version of programs and data files is used during the process.

Category	Control Activity •
	Programs include specific iterations to verify that the correct version of the computer file is being used during the process. • Programs check internal file header labels before processing. It includes specific routine procedures to achieve this. • Application protection against simultaneous file updates provides.

KF Appendix 2: Benefit-Cost Analysis Examples

Examples of Cost-Benefit Analyses to Use in Deciding on Adopting a New Control Activity

Example 1

You are considering hiring a Financial Services Assistant to perform 100% control over all payments made by spending units to ensure the correct amount is paid (they will conduct pre-financial checks before payment).

You anticipate that this task will take up 100% of the specialist assistant's working hours.

The cost of an expert assistant is 2,500 TL per month.

Scenario A

Benefit: The experience you gain from such a check-up will earn the expert assistant an average of 3,000 TL per month. It will find an overpayment error.

Decision – This inspection activity is cost-effective, and an expert assistant should be hired to carry out this inspection.

Scenario B

Cost: As above

Benefit: The experience you gain from such a check-up will earn the expert assistant an average of 2,000 TL per month. It will find an overpayment error.

Decision – This audit activity is **not** cost-effective, and an expert assistant should not be hired to perform this audit. You can instead focus on other audits.

Example 2

You do not currently have a public relations specialist.

In cases of lack of control in press relations, the risk of reputational damage has been identified with a high probability and high impact.

The cost of a public relations specialist is 4,500 TL per month.

Scenario A

You have a low risk appetite for reputational damage and believe that managing your press relations through a specialist will successfully reduce your risks to within your risk appetite limits (by significantly lowering the likelihood of reputational damage caused by false or misleading comments to the press). You believe this risk reduction is significant enough to justify employing a public relations specialist for your organization.

Decision: You are hiring a public relations specialist.

Scenario B

You have a high risk appetite for reputational damage, and you believe that the risk of reputational damage caused by false or misleading comments to the press without a public relations specialist is equal to or less than your risk appetite. Therefore, you believe that the cost of employing a specialist outweighs the benefit. Thus, you conclude that employing a public relations specialist is not cost-effective.

Decision: You are not employing a public relations specialist.

Action: Since your risk is equal to or lower than your reputational risk appetite, you do not need to identify an alternative control activity. However, you should continue to monitor the risk in the future, as you may need to change your decision if your risk appetite decreases or your probability and/or impact assessment of the risk increases.

CHAPTER FOUR

INFORMATION AND COMMUNICATION

1. INTRODUCTION

Information and Communication, the fourth of the five components of the Public Internal Control Standards, provides a link between the control environment, risk assessment, control activities, and monitoring through information sharing and communication. By regulating the flow of information

throughout the administration, it plays a significant role in increasing the functionality and applicability of the internal control system, which is seen as a tool for achieving corporate aims and objectives.

The purpose of this section of the guide is to provide information on the structures and practices related to the use of information and communication mechanisms within the framework of public internal control standards, so that administrations can carry out their activities in line with their objectives and ensure accountability; and to provide guidance to users on reporting, record-keeping and filing systems, and methods that can be followed for reporting errors, irregularities and corruption. **Communication** refers to the transmission and transformation of information, both horizontally and vertically within the administration and through appropriate mechanisms outside

the administration, to relevant individuals, administrations and authorities. Administrations should aim to establish an effectively managed and well-coordinated communication system to provide managers, employees and the public with the information they may need.

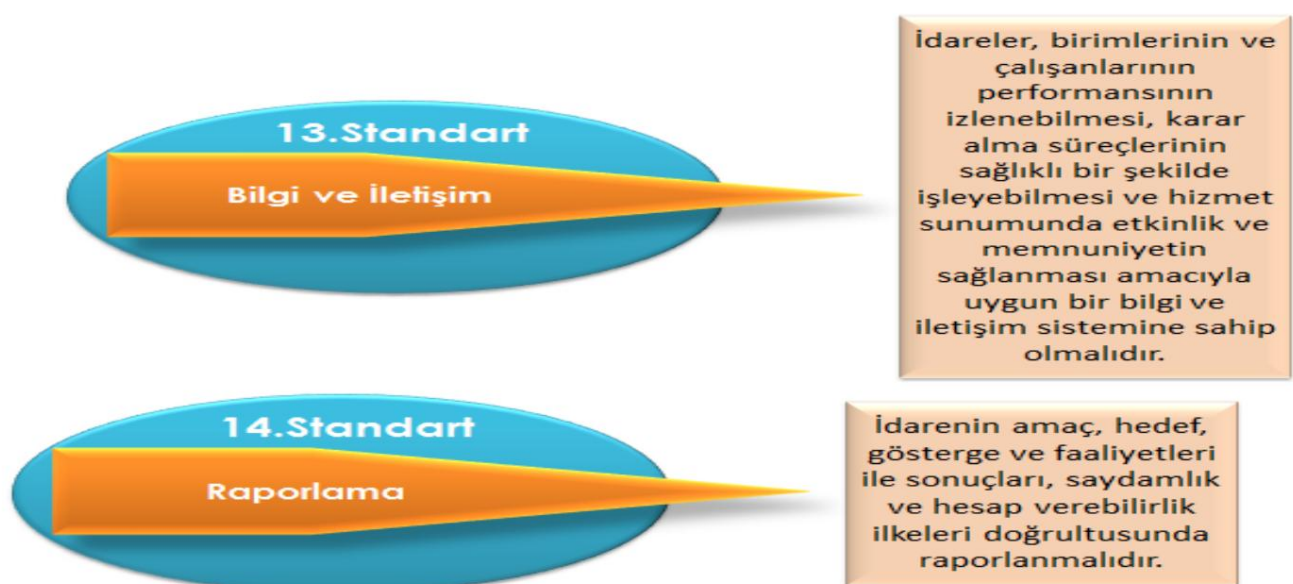
If information communication systems do not function properly, managers and personnel may face risks such as being unable to make timely and accurate decisions, being unable to implement them, and ultimately failing to achieve desired goals. Therefore, information must be accessible, useful, timely, accurate, complete, and up-to-date.



2. INFORMATION AND COMMUNICATION STANDARDS

Information and communication encompasses an information, communication, and record-keeping system that ensures necessary information is transmitted to those who need it—personnel and managers—in a specific format and within a timeframe that allows stakeholders to fulfill their internal control and other responsibilities.

BI Box 1: Information and Communication Standards





3. ROLES AND RESPONSIBILITIES IN INFORMATION AND COMMUNICATION

3.1. Senior Executive

The senior manager shall inform all units, via the internal electronic communication network or through official written notice, about the strategic plan, performance program, activity report, and RSB preparation that must be prepared in a way that will enable the achievement of predefined goals in the areas for which the administration is responsible. They should make a general announcement about what needs to be done before starting their work.

Furthermore, since the quality and nature of information and communication between senior management and other stakeholders directly affects senior management's accountability, senior management should guide relevant units on the frequency and methods of feedback. When establishing and integrating new information systems, senior management

should evaluate whether existing information systems meet the needs, taking into account the opinions of spending units, the General Directorate of Security, and the internal audit unit. If a new system is established, it should be designed with integration with other information systems in mind.

3.2. Internal Audit Unit

As part of internal auditing, a report is submitted to senior management on whether the administration's internal control system is functioning fully and accurately. To fulfill these tasks, the internal audit unit must have unrestricted access to all necessary information.

Based on the reports submitted by the internal audit unit, senior management may request spending units to develop preventive or corrective control activities, or may request additional reports.

3.3. Spending Authority

Spending authorities must ensure that duties, authorities, and responsibilities are clearly defined in writing and communicated to all personnel.

Within this framework, a task distribution chart showing the functional reporting network should be created and communicated to the personnel; and a communication network should be used to ensure that managers and personnel have quick and timely access to the activities carried out and their results.

Spending authorities;

- To ensure the accurate and reliable acquisition, storage, and transmission of necessary information regarding the objectives, activities, and indicators relevant to its own unit, as outlined in the administration's strategic plan and performance program, by effectively utilizing an electronic communication and archiving system.

- Regularly announcing the performance targets and indicators for their units, as well as the status of their tasks and activities and the basis for the data, on their unit's website.
- Data regarding periodic reports to be submitted to SGB (unit targets and risks) (information, status, etc.)

It must provide.

3.4. Implementation Officer

The information in the expenditure instructions, which is the responsibility of the implementing officers to prepare the payment order document, must be complete, accurate, understandable, and reliable. This plays an effective role in enabling the implementing officers to perform their duties correctly and as required. Therefore, implementing officers should inform the spending authority about the expenditure process at regular intervals.

3.5. Accounting Officer

They are responsible for the proper, transparent, and accessible maintenance of accounting services and records. Accounting officers must submit periodic reports to the spending authority regarding accounting records.

3.6. Strategy Development Units

SGB (State Economic Enterprise) managers should hold periodic meetings with spending authorities from other units to evaluate the information contained in activity reports, performance programs, and strategic plans. SGB employees should obtain the necessary information in the field of financial management and control through these individuals. The necessary coordination for the formation of the team that will carry out the

establishment and development of the Management Information System (MIS) in the administrations should be provided by the SGB.

In fulfilling the coordination duties defined by law for Strategy Development Units, secondary and tertiary level regulations such as the Regulation on the Working Procedures and Principles of Strategy Development Units, the Procedures and Principles Regarding Internal Control and Preliminary Financial Control, the Strategic Planning Guide for Public Administrations, the Regulation on Performance Programs to be Prepared by Public Administrations, the Performance Program Preparation Guide, and the Budget Preparation Guide should be taken into consideration.

SGBs should have websites to perform their duties more effectively, and these websites should include sections such as best practice examples, forums, and frequently asked questions to facilitate communication with internal and external stakeholders.

3.7. Financial Management and Control Center Harmonization Unit (FMCU)

MYK MUB, in fulfilling its duties, operates in the field of information and communication;

- It creates a common network (web-based) where information can be shared. Within this framework, the necessary information regarding the internal control system is shared between SGB and MYK MUB.
- Training, panels, and events for actors and senior management involved in the field of internal control. It organizes conferences.
- To ensure information and communication with the SGBs (School Management Units) of the administrations, personnel responsible for the administrations are assigned within the MYK MUB (Vocational Qualifications Authority of Turkey). They provide information and consultancy to the SGBs through communication channels such as official letters, call centers, telephone, and forums.

Public administrations should consider the regulations in the legislation directly related to the field of information and communication, in addition to the practices and methods included in this Guide. For these regulations, see Appendix 1: Legislation in the Field of Information and Communication.

4. INFORMATION

The prerequisite for reliable and relevant information is the timely recording and proper classification of business and transactions. Internal control includes the acquisition, classification, recording, use, and reporting of both financial and non-financial information.

4.1. Properties of Information

Information used in public administrations must possess the following characteristics:

• Timely: Information must be obtained and communicated by the relevant personnel at the right time.
• Relevant: The information must be relevant to each activity, task, or action itself.
• Accessible: Information should be accessible to those who need it, both when and in the future. Users should be provided with the necessary technological means to facilitate the acquisition, storage, transmission, and use of information.
• Understandable: The information described should have the same meaning for users at all levels of administration. Furthermore, information shared with external stakeholders should be clear and meaningful to users.
• Available: The available information meets the needs of users in accordance with the purpose for which it was obtained. should meet.
• Complete: The content and format of the information must be complete in a way that ensures its effective and efficient use.
• Accurate: The information fully and truthfully describes matters relating to the purpose, objectives, and activities to which it relates. It should be able to reflect that.
• Up-to-date: Information must be relevant to users' needs and current. Outdated information can negatively impact decision-making and service delivery. Managers and staff should take necessary measures to keep information up-to-date.

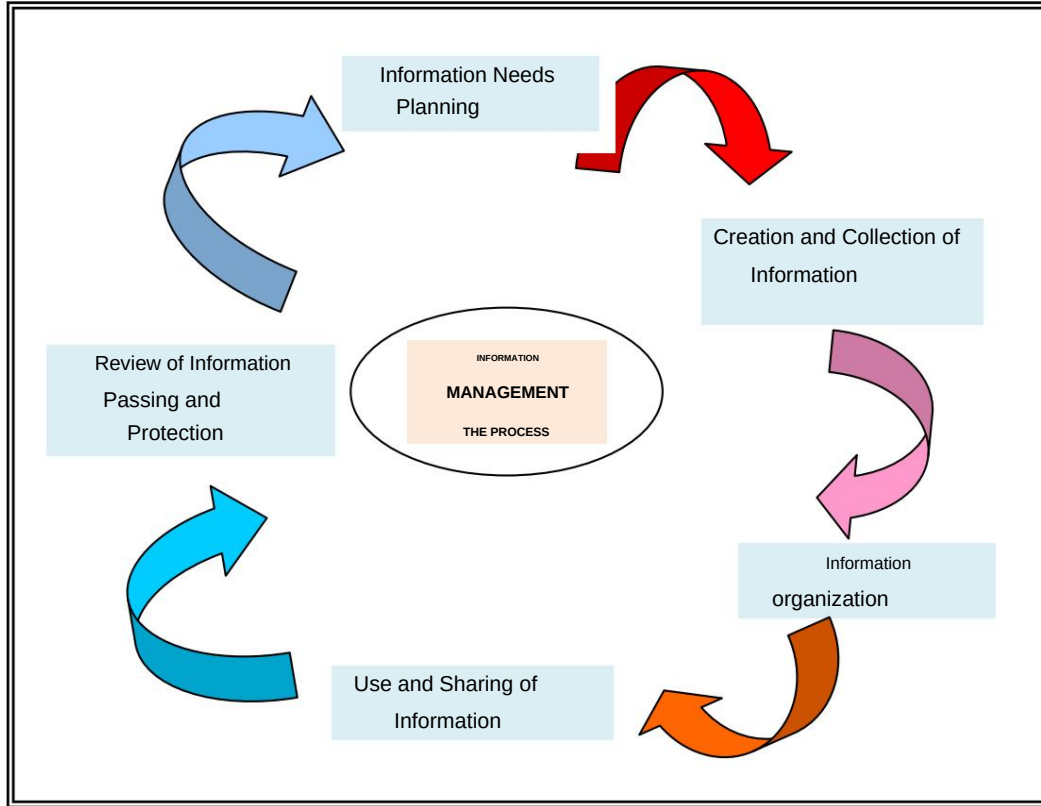
4.2. Information Management

Information management is the process of planning information needs, obtaining information from internal or external sources, classifying, storing, sending it to relevant places at the right time for interpretation, reviewing it for updating, and finally, discarding it.

The stages of the process are complementary, and at any stage it may be necessary to consider the steps of the previous or next stage.

The stages of the information management process (IMP) are shown in Figure 1.

Figure 1: Information Management Process



4.2.1. Planning Information Needs

Information needs planning involves strategic goals and objectives, performance targets, and this... It begins with identifying the information needs required to achieve the goals.

In order for the administration to carry out its activities effectively, from the strategic level to the operational level... in all stages, up to and including activities at the level of;

- whose, -
- what kind of information,
- When,
- from which sources and
- This includes assessing

the scope in which it will be needed.

The following points should be considered during the planning phase:

- Internal and external information users must be identified and classified. Users' information needs must be determined. Information stocks should be analyzed to determine whether users' information needs can be met with the available information.
- When planning new databases and information systems, the risk of information being leaked to the public should be considered. should be included.
- The value of the information to users and the cost of obtaining it should be analyzed.
- Information needs should be defined along with the relevant information system requirements; furthermore, what this study aims to achieve should be determined. The time and who will do it must be determined.
- Information needs should be compared with existing information and information systems both within and outside the organization.
- Information to increase the value or efficiency of existing systems, or to reduce their cost. Methods such as integrating systems, using new technologies, or employing standard practices can be employed.

4.2.2. Creation and Collection of Information

The creation and collection of information is essential for managers and staff to perform their duties.

It is about their ability to access the necessary and sufficient information in a timely manner.

At this stage, the value of the information from an administrative perspective should first be determined, and those who will need the information should be identified.

It must be ensured that people have access to information in a timely manner.

The following aspects should be focused on in the information gathering and creation process within administrations:

- The information collected or generated must be of a nature that can meet legal requirements and the needs of the administration and users. Continuing the collection of information that is no longer needed is prohibited. should not be done.
- The administration should determine from whom information will be obtained, how often and in what detail, and how much of a burden this process will place on individuals.
- Cooperation should be established with other administrations in matters such as sharing information or joint information gathering.
- If the administration stops collecting information, will any person or program be affected by this? It must be determined that it will not be affected.
- Information should be collected in information pools. This information should be clear and understandable; it should be classified and made available for use at the strategic and operational levels, in accordance with the information hierarchy. The management of the information pool should be carried out by an authorized team within the administration that is familiar with the established processes.
- Information gathering must be coordinated. Information gathering activities should be described to include all units, and the collected information should be publicly available. • The administration must ensure that the information gathering process complies with existing standards.
- Existing information stocks (in paper or electronic format) should be reviewed to ensure that the needs are met. It should also be determined who will perform this task.

The main sources from which information will be gathered are:

- Instructions, approvals, payment order documents, receipts, petitions • Information between service users, suppliers, or other public administrations and units and documents
- Plans and programs, budget proposals, estimates, work/business plans/operational plans, • Drafts, job descriptions,
- Reports, summary notes, policy, rationale and other documents supporting activities, • Meeting documents, agenda and records of decisions
- Commission documents, minutes, list of members
- Information requests and responses, emails, response forms
- Templates, relevant instructions, completed answers in all formats
- Beneficiary records, applications, evaluations, telephone interviews • All types of data in a computer environment
- Other sources.

4.2.3 Organization of Information

The organization of information involves establishing a relationship between the use, sharing, archiving, and destruction of information and the activities of the administration, and facilitating this process and access for the administration and other stakeholders.

The following points should be considered in the effective organization of information: • Administrations

should have comprehensive and up-to-date systems in place where all documents, transactions, and processes are recorded, classified, and filed in accordance with established standards.

- User satisfaction regarding access to information should be ensured both within and outside the administration. Methods for measuring user satisfaction should be determined. (Such as surveys conducted after the completion of specific services or periodically)
- Information to be conveyed to the public must be presented in an appropriate place, time, and manner. (Such as establishing structures that facilitate public access, such as using websites or e-libraries.)
- Units responsible for information stocks and the provision of services related to information processing infrastructure (IT departments, library services, etc.) should identify users' information needs; they should improve their services to better meet user needs and provide easier and faster access. (Such as shortening response times, using efficient technology for information transmission, and designing a user-friendly system.)
- Information that can also be used by other public administrations is subject to legal limitations.
It should be checked whether or not this is the case.
- Administrations should classify their publications, if any, according to established standards, store them up-to-date (in their libraries and electronically), and provide access to them.
- Appropriate documents published by the administrations can be made available on the administrations' websites.
It should also be included on the pages.

4.2.3.1. Recording, Filing and Archiving Information

a. Record Keeping and Filing

Establishing a robust information and communication system requires the recording, classification, filing, and archiving of all incoming and outgoing documents, internal communications, and business transactions, including those in electronic format, and these services must be provided through a comprehensive and up-to-date system.

These documents should be easily accessible when needed.

The registration process, including the initial and approval stages, should be continued throughout all processes of the business and transactions, up to the final classification. This also applies to the regular updating of all documents.

Public administrations must adhere to the Prime Ministry Circular No. 2005/7 on the Standard File Plan, published in the Official Gazette dated March 25, 2005, and numbered 25766, when filing documents created electronically or in physical form.

Regardless of the medium from which they are received (such as paper, fax, email, or electronic media), all documents must be recorded and maintained in an official file or electronic format, according to an appropriate record-keeping plan. These procedures must be communicated to employees in writing.

With standardization in filing services;

- This will ensure that documents on the same subject are coded with the same numbers in public administrations.
 - Since standard file numbers will represent the same subject in all public administrations, the required information and documents can be accessed easily, accurately, and quickly, and it will greatly facilitate the sorting, classification, placement, and accessibility of documents in archives.
 - This will ensure consistency and ease in establishing a regular, fast, effective, and efficient document, file, and communication system among administrations.
 - It will provide the infrastructure for the automation of documents and correspondence between administrations and the creation of information networks.
 - Internal and inter-institutional document and task tracking will be facilitated. •
- The required document or information can be easily found more quickly among documents bearing the same number.
It can be found.

The task of working on the recording, use, and archiving of electronic documents was assigned to the General Directorate of State Archives by the E-Transformation Executive Board on September 9, 2004, in accordance with the Prime Ministry's Circular No. 2008/16 on Electronic Document Standards, published in the Official Gazette No. 26938 dated July 16, 2008. This led to the publication of the TSE 13298 standard. This Decision number _____ standard serves as a fundamental resource for electronic document management systems to be used by public administrations.



Electronic document management systems created by administrations must operate in accordance with the TSE 13298 standard, and the sharing of generated electronic documents between institutions must be carried out according to the inter-institutional electronic document sharing service criteria specified on the website www.devletarsivleri.gov.tr.

b. Archival Services



Archival services include identifying materials held by administrations and individuals that will later become archival material, ensuring that these materials are not lost for any reason, guaranteeing their preservation under necessary conditions, evaluating them in accordance with national interests, and sorting and destroying materials that are not deemed necessary for preservation.

The procedures and principles regarding archival services are regulated in the Regulation on State Archival Services, published in the Official Gazette dated May 16, 1988, and numbered 19816.

According to this Regulation, administrations must take measures to ensure that their information and documents are adequately protected against theft, fire, flood, and other disasters; determine the rules for how to handle confidential documents; take necessary precautions to ensure that documents remain readable in the future; and inform management and personnel about appropriate retention periods for information and documents.

4.2.4 Use and Sharing of Information

The use and sharing of information is crucial for ensuring accountability and transparency among those involved in the administration's activities and other stakeholders, as well as for guaranteeing the continuity of operations.

Information is renewed and gains value as long as it is transmitted and shared. In information management, corporate knowledge is also about knowledge within the organization and Regular transmission and sharing of information is essential. Corporate information sharing is a cycle consisting of delivering information to relevant individuals and authorities, keeping them informed of the work, receiving and evaluating feedback, and transmitting it again.



The following points should be considered when using and sharing information:

- Adherence to privacy, security, and legal restrictions.
- If possible, use electronic means to share information resources (email, information pools, websites, etc.).
- The information must be complete, accurate, up-to-date, relevant, and understandable.
- Verifying the accuracy and reliability of the information (especially when conducting web-based research).
- Consideration of copyright, licensing, and intellectual property rights. • Institutional investments in information resources (journal subscriptions, databases, online (such as services) to benefit from.
- The source of the "transferred" information must be indicated, regardless of whether it is taken from a source in the existing institutional knowledge pool, a publication, or a website.

On the other hand, internal information sharing and control are aimed at ensuring the continuity of operations. It also supports their activities.

For example, the issue of information transfer between personnel leaving their positions and those newly starting their duties should be evaluated by the administrations, and necessary measures should be taken. In this context, the suggestions in Table 1 of the Information Management System can be taken into consideration.

Table 1: Procedures to be Followed in Case of Resignation and Appointment

Departure from Position • Review	New Job Appointment Status
and monitoring of job descriptions and work processes upon departure from the position, • Departing personnel should provide their replacements with all relevant job information, including an explanation of why they are needed, a summary of ongoing tasks, a list of job-related contact information, and an inventory of information sources (including file numbers). • Backing up all transaction-related information in electronic format and transferring it to an information pool, • Under responsibility Ensuring the relating to transfer of files to personnel.	• Defining and notifying the new staff about their duties, • Information in electronic or paper form • Regarding access to electronic devices: checking whether the source has been transferred to him/her noting down the instructions and notifications received, • Ensuring that new personnel become familiar with information management responsibilities and practices, • Including new staff in training on information management and record keeping.

4.2.5 Review and Protection of Information

Administrations should periodically evaluate the fundamental processes involved in information management, such as planning information needs, creating, collecting, identifying, defining, using, and sharing information, and the results should be shared with managers. Information must also be protected against loss, unauthorized access, use, alteration, and destruction.

The following points should be considered for this:

- Storing information in a way that preserves its form, structure, scope, and content.
 - Classifying information and documents, whether in paper or electronic form, according to appropriate security and confidentiality classifications.
 - Ensuring that protected information is only accessible to those authorized to access it. Implementation of control procedures.
 - The level of protection should be consistent with the risk level, •
- Other user requests for access and use should be taken into consideration and comply with legislation. Assessment of suitability.
- Backing up the data at regular intervals.

The value of information determines not only how it is used and protected, but also when and how it is destroyed. Legislation, information policies, and needs can influence how long information should be retained. Protected information must be destroyed in accordance with relevant legislation and with the necessary approvals.

4.2.5.1. Information Security

The purpose of information

security is to:

- Protect the integrity of information,
- Protection of privacy (prevention of unauthorized access),
- Ensuring availability and system continuity.



Information can be in written form, stored electronically, or verbally communicated between individuals. Regardless of its form, information must be properly recorded, protected, and backed up, whether in paper or electronic form. Information security refers to preventing the loss, misuse, and damage of valuable information assets within an administration.

4.2.5.1.1. Information Security Management System

An Information Security Management System is a systematic approach adopted by an administration to properly manage sensitive and critical information it possesses. The primary goal of this system is to protect, store, and make available, when needed, information deemed sensitive and critical by the administration.

a. Information Security Management System Installation

For the establishment of an information security management system:

- Limits on whether the system will cover the entire administration or only a part of it. It must be determined.
- A policy that sets out the objectives should be established.
- A systematic risk assessment approach should be adopted, potential risks should be identified and mitigated appropriately.

In this context, the "Information Security Management System Setup Guide" prepared by the Turkish Scientific and Technological Research Institution National Electronic and Cryptology Research Institute and published on the website www.bilgiguvenligi.gov.tr can be reviewed. While all personnel have a responsibility to show the necessary attention and care in

ensuring the information and system security of the administration, the information processing units of the administration/spending units are responsible for making the necessary arrangements and determining policies in this area, in cooperation with the relevant units when necessary. **b. Security Controls/Principles**

To protect the security and confidentiality of information stored electronically, security controls and principles must be established in the face of malicious attacks and resulting vulnerabilities. The absence or inadequacy of these controls can lead to vulnerabilities (such as hacking), significantly reducing the effectiveness of the information security system.

The fundamental security principles are confidentiality, integrity, availability, accountability, and access control.

5. MANAGEMENT INFORMATION SYSTEMS (MIS)

MIS provides managers with the strategic information they need to make decisions, as requested.

These are computer-aided systems (consisting of software and hardware) that enable the presentation of information.

Management Information Systems (MIS) aim to deliver accurate and complete information to the right people in the appropriate format (forms, reports, tables, graphs, etc.). In this context, they evaluate the administration's financial data, personnel information, movable/immovable asset information, performance data, information in the corporate document archive, etc., by comparing them. They can also provide the administration with information on risk management.

Some administrations have scattered information systems; however, the existence of these structures does not mean that those administrations have Management Information Systems (MIS). Data recorded in different units and systems is stored independently of other units. Information duplication across different units of the administration leads to inefficient use of resources. MIS enables administrators to access information encompassing the entire administration by entering data into a central computer system.

On the other hand, resistance to information sharing within administrations is a significant problem. Since administrators in administrations where information is not shared cannot access the information they need completely and in a timely manner, this constitutes a major obstacle for Management Information Systems (MIS). Therefore, a culture of information sharing should be created and supported within the administration.

5.1. MIS Setup Stages

In designing an Information Security System (ISS), it is essential that personnel understand the importance of obtaining and recording reliable and accurate information, and are aware of their responsibilities in this area. Secondly, the business processes related to information production must be fully and clearly defined, and finally, support from information technology should be utilized in this field.

Article 15 of Law No. 5436 assigns the task of providing services related to management information systems to Strategy Development Units (SGBs). Furthermore, the Regulation on the Working Procedures and Principles of Strategy Development Units states that, if applicable, carrying out services related to management information systems in cooperation with relevant units and conducting system development efforts are among the duties of SGBs.

In this context, services for the establishment and development of the MIS should be carried out by creating expert/support units within the SGBs (Sectoral Development Units), in cooperation with the IT units if any, and with the participation of the spending units. During the MIS establishment phase, SGBs and spending units can follow the processes

below: 5.1.1. Establishment of the MIS Working Team

In establishing Management Information Systems (MIS) in administrations, a participatory approach should be adopted, and a team should be formed under the coordination of the SGB (Sectoral Management Board) with the participation of representatives from all spending units to determine the work program and assign tasks.

5.1.2. Planning and Execution of the MIS Setup Activities

In the efforts to establish the MIS (Minimum Behavioral Information System):

- First, to determine what kind of information the administration might need, a comprehensive assessment will be conducted across the administration. A comprehensive needs analysis should be conducted.
- Next, it is necessary to identify the units that provide data to the MIS. This identification will be created. This will create an important infrastructure for the information map.
- The current situation regarding the characteristics of the administration's information systems, the problems related to them, and proposed solutions should be presented; actions to be taken to solve the problems and objectives should be determined. In this context, mechanisms should be established to support the production and sharing of information.
- The benefits and cost aspects of the proposed system should be presented.
- Risks that may arise in connection with the establishment of the MIS should be identified and a risk management process should be implemented. Control activities to be applied against risks with a high level of importance and probability should be determined.
- The system's success criteria must be defined. (It must adapt to changes within and outside the administration.) (such as being flexible and including early warning mechanisms)

In the medium term, it would be appropriate to create an "organizational knowledge map" across the entire administration. This would allow for quick access to the necessary information and expertise. The knowledge map should be created first at the unit level, and then at the employee level according to the expertise and experience of individuals. In creating such a structure, the administration's organizational chart and the division of labor within lower-level units can be utilized. Once the organizational knowledge map is created and operational, the following question can be easily answered: "Who knows what?" For example, who possesses personnel information, budget information, or archive information.

(which department, which staff member, etc.) and the relationship between this information can be determined as quickly as possible.

The establishment phase of the Management Information System (MIS) can begin with pilot applications in the units. Starting with pilot applications and determining how the system works will save time, cost, and labor. By addressing the shortcomings observed in the pilot applications and taking measures to correct errors, potential mistakes in later stages of the process can be prevented.

5.1.3. Monitoring and Evaluation of the MIS Setup Process

Periodic reports should be prepared and submitted to senior management to show the progress of the work and activities carried out during the establishment of the Management Information System (MIS) and the development of the system. At this stage... Measures should be taken against any identified shortcomings, and activities should be carried out as planned. Furthermore, the audit results and evaluations conducted by the administration's internal auditors on the system and its outputs should also be considered.

Management Information Systems (MISs) need to be kept dynamic at all times, adapting to both technological advancements and changes and diverse demands in the knowledge areas required by management.

6. COMMUNICATION

Communication is the sharing or exchange of information between individuals, units, and/or administrations for purposes such as service delivery, supporting and sharing decisions, and carrying out and coordinating activities within the framework of aims and objectives. It plays a key role in decision-making by providing feedback to management in the development of a healthy internal control system.

Communication can be internal, external, verbal, written, or electronic. Where verbal communication is deemed sufficient, only the important information conveyed verbally needs to be documented.

In this way, a record of important information is kept for later use by those who are granted access authorization.

BI Box 2: Essential Characteristics of Effective Communication Channels

• It provides accurate information at the right time.
• It meets individual needs.
• Informs employees about their roles and responsibilities.
• Supports reporting.
• It provides employees with the opportunity to make suggestions for improvement.
• It conveys clear messages to senior management, enabling them to make informed decisions.
• It informs employees about the importance of internal control and decision-making.
• It is directed both internally and externally.
• Target audiences have been accurately identified.

It would be appropriate for administrations to establish communication channels possessing the essential qualities mentioned above.

6.1. Internal and External Communication

In administration, information is needed at every level to achieve objectives and manage related risks. Within the scope of internal communication, information should be conveyed to managers and/or personnel who need it, in a timely and appropriate manner, so that they can fulfill their responsibilities and ensure coordination between the decisions and activities of different units.

Accordingly, information flow occurs "**horizontal**" between the same hierarchical levels within the administration.

Communication can take the form of "vertical communication" and "internal communication" that occurs between different hierarchical levels.

External stakeholders such as service users, suppliers, and other public administrations.

Communication is also essential for effective internal control.

Administrations should consider the following general principles in internal and external communication:

- Governments must provide the public with timely, accurate, transparent, objective, and complete information about their policies and programs, services, and activities.
- Clear and simple Turkish should be used.
- Administrative bodies should be transparent, accessible, and accountable in the services they provide.
- Numerous tools and methods related to communication should be used to meet different needs, Information from different fields should be utilized.
- Communication needs should be identified regularly.
- Administrations should seek the opinions of internal and external stakeholders in determining their aims and objectives and in establishing their processes, and should create mechanisms to ensure that these opinions are evaluated.
- It should cooperate when necessary to ensure effective communication with stakeholders.
- Administrations should develop the capacity and equipment to follow technological innovations and applications in the field of communication and allocate appropriate resources for this purpose. In this context, activities should be proportionate to the allocated resources and expected results.

Table 2 of the BI document outlines some internal and external communication principles and methods.

Table 2: Communication Principles and Methods

INTERNAL	
Communication	Method
Principles: Senior management and employees must understand the internal communication system and be aware of their responsibilities within it. Internal communication activities and processes should be monitored at regular intervals, revised as needed, and new communication methods should be determined to suit the changing administrative structure. Employees should be able to communicate their evaluations, suggestions, and problems to senior management.	The administration should regularly inform employees in writing or electronically about the functioning of the internal communication system, tasks, and responsibilities. Mechanisms should be established to communicate the administration's mission, vision, goals, and specific objectives, within the framework of their duties and responsibilities, to all personnel. (intranet, internet, bulletin boards, executive briefings...)
Communication between managers and employees should be open and collaborative, aimed at achieving the administration's goals and mission. The individual and the staff's goals are aligned with the administration's objectives. They need to be able to combine their goals.	Regular meetings and keeping communication channels open so that employees' ideas and suggestions are listened to and considered. Organizing internal communication seminars and training programs.
Personnel must provide management with the information it needs to make decisions and achieve administrative objectives in a timely, complete, and accurate manner.	Within the administration, a reporting system that operates from personnel to managers regarding activities and processes (meeting minutes, unit activity reports, information exchange of verbally or electronically)

For this purpose, personnel should be informed by their manager of when, to what extent, by what method, and from which unit the information is requested. Managers inform staff about the administration's policies The And and objectives. purpose should be to inform.	(a continuous system, such as a reporting system that allows the manager to monitor daily activities). Announcement and monitoring of the administration's strategic plan, performance program, and unit operational plans.
Mechanisms should be established to ensure effective information sharing among employees at the same hierarchical level. The job descriptions of personnel and units required to share information must specify this, and this must be communicated to the personnel.	Organizing regular meetings among managers to share ideas and discuss issues and suggestions related to their areas of responsibility and management. Establishing a system to monitor meetings and activities among employees at the same level. Creating email groups for each hierarchical group.
Managers and relevant personnel should have timely access to the performance program and budget implementation, as well as other information regarding resource utilization.	Performance Programs, say2000i, e-budget, Unit and Administrative Activity Reports.
EXTERNAL	
Communication Principles	Method
Citizens' access to information from public administrations Access to services should be increased. Institutions by Services offered within the scope of e-government should be made accessible to citizens and other administrations as needed (MERNIS, UYAP, etc.).	Creating an administrative website to provide access to necessary documents and offering certain services 24 hours a day through this website. Regular updating of documents and data related to online services, and designating individuals within the administration responsible for the design and content of the website. Additionally, the content will be published in English to enable foreign users to access the information. Creating mechanisms (such as forums, frequently asked questions, activating the B�MER [Prime Minister's Communication Center] and the Information Access System] where citizens can submit their requests and complaints regarding administration and/or services, and obtain the information they need.
Governments should inform the media on matters that are important to decision-makers and the public.	Inviting the media to important conferences and seminars. The service offered by the administration is via television or Shown online as a promotional video. The senior management should inform the public annually about the administration's performance program and activity report, and these documents should be published on the website. Ensuring that the Press and Public Relations Units function effectively.

7. REPORTING

Reporting is an important tool for establishing an effective internal control system and, in particular, for facilitating monitoring activities.

Managers consider the reports presented to them when making decisions. In this context, accurate, concise reports will make the managers' job easier. On the other hand, communication and reporting are important elements of risk management and monitoring.

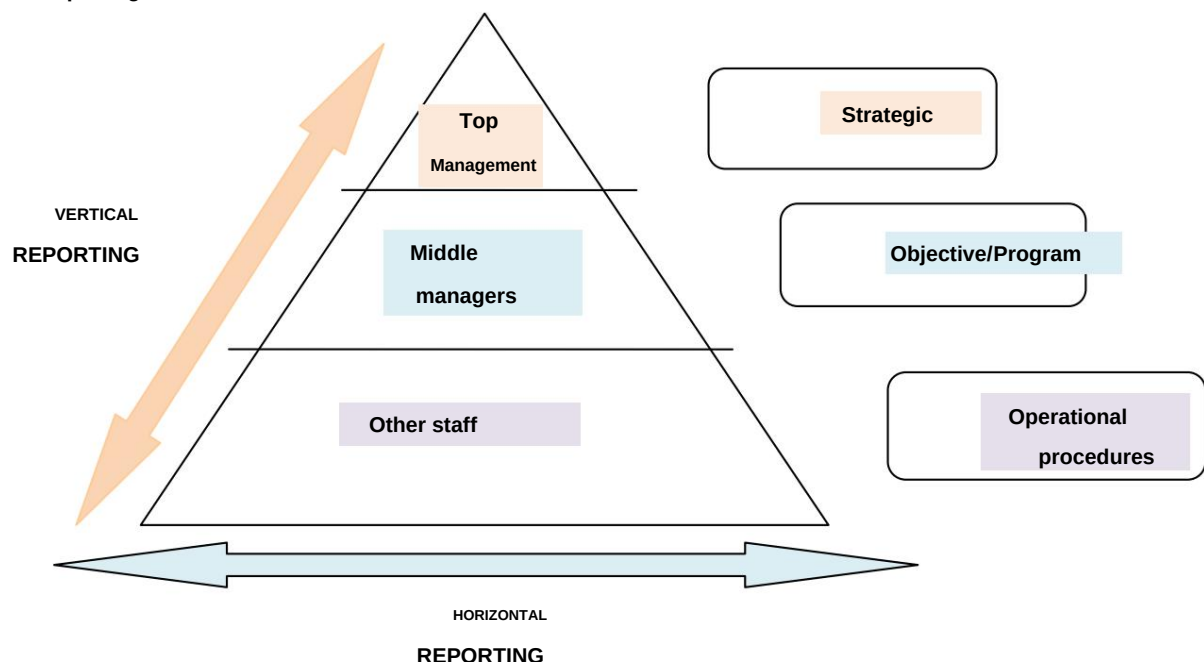
Administrations must report financial and non-financial information and results regarding their policies, programs, activities, and projects to relevant individuals and authorities in writing or orally at specified times. In this context, horizontal and vertical reporting networks within the administration should be established in writing. Furthermore, each administration should also consider external reporting mechanisms.

Figure 3 illustrates the vertical reporting mechanism between hierarchical levels and the horizontal reporting mechanism among personnel at the same level regarding strategic, programmatic, and operational-level decisions and actions within administrations.

Vertical reporting is the type of reporting that employees do to their managers.

Horizontal reporting is the necessary flow of information between individuals and departments at the same level.

Figure 3: Reporting Network



An example of internal horizontal reporting:

- The report that personnel participating in a training program will prepare regarding the training results. sharing it with colleagues.
- Meeting minutes shared with other units.

An example of internal vertical reporting:

- Consolidated Risk Report presented to senior management
- Monitoring reports of the Action Plan for Compliance with Public Internal Control Standards
- Meeting minutes submitted to senior management
- Internal audit reports submitted to senior management
- Quarterly/six-monthly activity reports submitted to senior management
- Domestic/international internship reports

Examples of external reporting:

- Internal Control System Evaluation prepared by SGBs and sent to MYK MUB
The report
- Prepared by the senior executive and announced to the public, submitted to the Court of Accounts and the Ministry of Finance.
annual activity reports, copies of which were sent

It can be shown.

BI Box 3: Essential Requirements for Effective Reporting

- It must be clearly defined and communicated to personnel which reports will be prepared, by whom, how often, when, to whom they will be submitted, their basis, and who will review the prepared reports. The reports must be consistent with the principles of financial transparency and accountability.
- The information contained in the reports must be accurate, up-to-date, unbiased, complete, relevant, and sufficiently detailed.
- Reports should use common and clear language that everyone can understand.
- Reports should be prepared periodically and on time, and comparisons should be made over the years.
It should enable it to do so.
- The report should be quick and easy to read, with a well-designed format and page layout that will capture the reader's attention, and should include sufficient and appropriate visual materials.
- In addition, all reports should include a conclusion and evaluation section.
- The format of the requested report should be determined in advance by the requesting administration/unit and communicated to the relevant administration/unit.

8. REPORTING IRREGULARITIES AND CORRUPTION

One of the key elements of accountability and transparency is ensuring that employees and stakeholders have an effective say. The key is to have a mechanism that will allow them to express their concerns in this way.

Article 279 of the Turkish Penal Code stipulates that a public official who, in connection with their duties, learns of the commission of a crime requiring investigation and prosecution on behalf of the public, and who neglects or delays in reporting this to the competent authorities, shall be deemed to have committed a crime.

8.1. Concepts of Irregularity, Corruption, and Whistleblowing

Irregularity refers to any act or omission that results in a violation of existing rules; corruption refers to administrative personnel or third parties intentionally acting in a manner inconsistent with existing rules in order to obtain an unfair or unlawful benefit.

Whistleblowing is the act of informing relevant units or individuals about illegal and unethical behavior and actions within the administration, in order to prevent harm to the administration or third parties or institutions outside the administration.

In this context, administrations are informed of irregularities, corruption, and errors, and It should define and announce methods for evaluation.

8.2. Scope of Notifications

In public administrations, complaints and reports may cover three main aspects:

- Reports and complaints regarding violations of ethical values.
- Reports and complaints regarding irregularities and corruption
- Complaints by civil servants regarding administrative actions and procedures applied to them by their superiors or institutions.

Below are the essential information regarding these notification fields and related regulations.

8.2.1. Reporting and complaints regarding violations of ethical values: The

reporting mechanisms are specified in Law No. 5176 on the Establishment of the Public Officials Ethics Board and Amendments to Certain Laws, and the Regulation on the Principles of Ethical Conduct for Public Officials and the Application Procedures and Principles.

Accordingly, applications are submitted to the Ethics Committee in cases where the general director and public officials holding titles considered to be at this level violate ethical conduct principles, while applications regarding other officials are submitted to the Ethics Committee. In cases of violations of ethical conduct principles, the matter will be referred to the relevant institution heads for referral to the competent administrative disciplinary boards. Within this scope, administrations will implement the process to ensure compliance with the legal provisions.

8.2.2. Complaints regarding irregularities and corruption

There are numerous regulations regarding reports of irregularities and corruption. For example, Law No. 4483 on the Trial of Civil Servants and Other Public Officials specifies the procedures to be followed regarding crimes committed by civil servants and other public officials in the course of their duties. Accordingly, the making, processing, and conclusion of a report or complaint against civil servants and other public officials will be carried out within the framework of the aforementioned Law. On the other hand, the "Strategy for Increasing Transparency and Strengthening the Fight Against Corruption (2010-)" published by the Prime Ministry in the Official

Gazette dated 22/02/2010 and numbered 27501,

In 2014, measures were included at the national level to prevent corruption, implement sanctions, and raise public awareness.

Furthermore, the "Guidelines on Reporting Corruption," published in 2009 by the Prime Ministry, the Ministry of Justice, and the Public Officials Ethics Board, contain the relevant legislation and fundamental principles, and it would be appropriate for administrations to take these principles into account in their work regarding the whistleblowing system.

8.2.3 Complaints to be Made by Civil Servants

Civil servants shall be subject to administrative actions and procedures implemented by their superiors or institutions in accordance with Article 21 of Law No. 657 and the Regulation on Complaints and Applications of Civil Servants prepared based on this article.

8.3. Responsibility in Detecting Errors, Irregularities and Corruption

The responsibility for preventing and uncovering errors, irregularities, and corruption lies with the administration and all administrative personnel. Within the framework of an ethical conduct culture within the administration, those responsible for management must take the necessary measures to prevent errors, irregularities, and corruption under their supervision.

8.4. Reporting System

The procedures and principles included in the regulations mentioned above contain separate procedures depending on the subject and method of reporting. When developing their reporting systems, administrations should take these regulations into account and have internal regulations in place that allow employees and third parties to submit reports, in accordance with their own institutional structures and reporting mechanisms. These regulations should include:

• What can be reported, • How the
safety and confidentiality of a well-intentioned whistleblower will be ensured,
• The stages through which a report can be made within the administration (in order: first-line supervisor, unit head, internal audit unit head, or human resources unit head, or financial services unit head, senior manager),
• How the reports received will be evaluated by the administration and what actions will be taken (such as an internal review or official investigation),
• The whistleblower should be informed of who is handling the case, whether they can be contacted, and the evaluation and/or results.

should be included.

In this context, administrations should inform all personnel about the procedures for reporting and filing complaints, ensure that the identity of personnel is kept confidential in possible reports and complaints, and prevent discriminatory treatment of personnel as a result.

While written notifications are the primary method, administrations should enable electronic complaints and notifications through various forms created on their websites. Furthermore, administrations should establish the necessary mechanisms to facilitate easier reporting and complaints from external stakeholders, and publish these on their bulletin boards and websites.

Administrations should not establish mechanisms other than the preliminary investigation procedures specified in Law No. 4483, especially in reports and complaints concerning corruption and irregularities. Regardless of whether an investigation is authorized or not as a result of the preliminary investigation, the situation, along with detailed justification, must be reported to both the Public Prosecutor's Office and the informant, and written records of this notification must be kept in the complaint files.

It is appropriate for administrations to consider the basic requirements in BI Box 4 for an effective whistleblowing system. will be.

Box 4: Essential Requirements for the Reporting Process

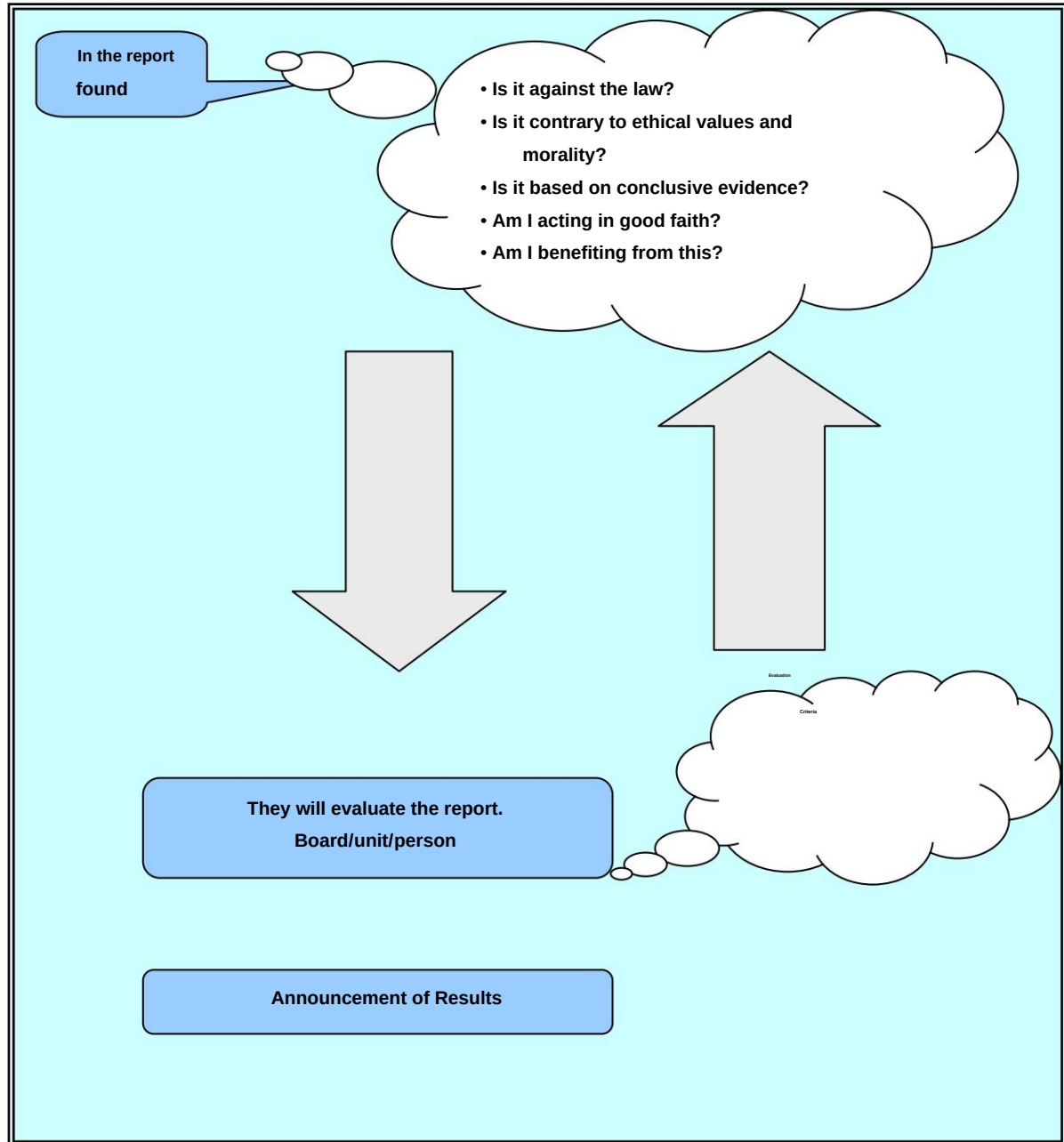
- Senior management should announce procedures for handling complaints and reports from both within and outside the administration.
- Administrations, both central and regional units, shall designate a unit or department to which reports will be submitted. They should identify and announce the individuals.
- Methods should be developed to enable personnel and third parties to provide information while keeping their names confidential (via telephone, forms published on the internet/website, petitions, complaint boxes, etc., in a way that allows for the submission of evidence).
- All reports, whether made verbally, in writing, or electronically, must be recorded sequentially by the unit or individuals to whom the report is made, using a separate folder or registration system.
- Discriminatory treatment of personnel who report wrongdoing should be prevented.
- Periodic meetings should be held with staff to gather their opinions; staff should be encouraged to report malpractice within the administration, and trust should be established.
- All communication channels should be kept open to enable personnel to report incidents.
- If the employee's report is found to be true as a result of the investigation and evaluation It should be determined by methods specified by the administration.
- Even if the report is not in accordance with proper procedure, it must be evaluated if it is based on conclusive evidence.

When evaluating reports, attention should be paid to the points in BI Box 5.

BI Box 5: Evaluating Reports

- Are the behaviors and actions observed within the administration against the law?
- Behaviors and events observed within the administration violate ethical values (general morality, work ethics, etc.). Is it against morality (etc.)?
- The seriousness and importance of the issues raised should be taken into consideration.
- Good faith and a public interest are necessary.
- There must be a reasonable belief that the information and the claims contained within it are entirely true and that it exposes wrongdoing.

Figure 4: Reporting Process



9. INTER-UNIT RELATIONS

9.1. Communication Between MYK MUB and SGBs

The degree of effectiveness and efficiency of MYK MUB in its duties depends on the quality of its communication with SGB.

The Vocational Qualifications **Authority (MYK MUB)** should develop institutional communication mechanisms for the transfer of information to the SGBs (School Management Units). These mechanisms could be established through a call center within the MYK MUB, or by each MYK MUB staff member assuming an institutional consultancy role for the SGBs of specific administrations.

Thus, the MYK MUB personnel will be able to familiarize themselves with the unit they are responsible for, make assessments specific to that unit, and generate information to solve problems accordingly, thereby increasing the effectiveness of the MYK MUB.

Furthermore, facilitating face-to-face communication between MYK MUB personnel and SGB personnel, and organizing periodic meetings and/or brainstorming conferences to evaluate the internal control system, can be implemented as methods for information transfer.

MYK MUB should identify critical regulations concerning SGBs using participatory methods, and for this, the participation of SGBs must be ensured. Furthermore, the level of participation of SGBs will strengthen the level of communication achieved.

9.2. Communication Between SGBs and Spending Units

In the preparation of strategic plans, performance programs, and activity reports, which are elements of public financial management, and in the implementation of compliance studies with Public Internal Control Standards, the task of coordinating among spending units has been assigned to the SGBs (Strategic Development Units). Therefore, effective institutional communication with spending units will ensure the smooth progress of the coordination process. Matching of SGB employees with spending units should be carried out.

Each staff member at the SGB (Spending Unit) must be in constant communication with the spending units they are responsible for and be able to periodically share the information they possess with the spending units. To ensure a consistent and accurate flow of information between the spending units and the SGB, personnel within each spending unit/subunit should be designated to maintain constant communication with the SGB.

Furthermore, these information flows should be evaluated periodically (recommended minimum monthly, maximum quarterly) through periodic meetings between spending authorities and SGB management, and suggestions for necessary measures and improvements should be presented at these meetings.

In SGBs (Sectoral Development Boards), when decisions concerning spending units need to be made, spending unit officials should be able to participate in these decision-making processes, depending on the level of the decision.



INFORMATION AND COMMUNICATION SECTION APPENDICES

Appendix 1: Legislation in the Field of Information and Communication

• Regulation on Principles and Procedures to be Applied in Official Correspondence
• Prime Ministry State Archives, published in the Official Gazette dated 16/05/1988 and numbered 19816 Regulations Regarding Services
• Regulation on Ethical Conduct Principles and Application Procedures for Public Officials
• Declaration of Assets published in the Official Gazette dated 15/11/1990 and numbered 20696 Regulations Regarding
• The Law on Complaints of Civil Servants published in the Official Gazette dated 12/1/1983 and numbered 17926. Regulations Regarding Applications
• Prime Ministry's Standard File Plan Circular No. 2005/7 dated 24/03/2005
• Prime Ministry Circular dated 19/03/2007 regarding the Public Officials Ethics Board
• Telegraph and Telephone Law No. 406
• Law No. 3071 on the Exercise of the Right to Petition
• Law No. 3628 on Declaration of Assets and Combating Bribery and Corruption • Law No. 4483 on the Trial of Civil Servants and Other Public Officials
• Complaints Regulation within the scope of Public Procurement Law No. 4734
• Law No. 4982 on the Right to Information
• Electronic Signature Law No. 5070
• Law No. 5176 on the Establishment of the Public Officials Ethics Board and Amendments to Certain Laws Law on it,
• Law No. 5369 on the Provision of Universal Service and Amendments to Certain Laws Law
• Law No. 5651 on the Regulation of Publications Made on the Internet and Combating Crimes Committed Through These Publications • Electronic Communications Law No.
5809

Appendix 2: Commonly Used Communication Methods

Vehicle	Aim	Advantages	difficulties
Meetings	• Information • Seeking Feedback • Joint Decision Making	• Relatively inexpensive • A method that people are familiar with • Contribution to a culture of participation • Open to discussion and dialogue • The possibility of finding solutions to problems if well organized.	• Difficulty in measuring the success and value of the method • There may be practical no results • If not managed well, a small group can dominate the meeting.
Reports	• Information • Seeking opinions • Decision making • Evaluation	• Provides the target audience with accurate information on the subject. • It facilitates the manager's decision-making. • Access to accurate, up-to-date, unbiased, complete, relevant, and sufficiently detailed information.	• Requirement for qualified employees • Time-consuming to produce
Brochure/ Periodic Broadcasting	• Information • Introduction	• Creative design possibilities • Understandable • Specific and broad target groups • Opportunity to establish long-term relationships with the target audience • Enables regular updates on the subject.	• Limited feedback • On the target audience difficulty in measuring the effect
Questionnaire/ Interview (letter, email, telephone, face- to-face meetings)	• Seeking Feedback • Evaluation	• A method that people are familiar with • It can reach a wide audience. • Ability to select a specific target audience • Scientific methods can be applied	• Expensive, time-consuming • In-depth knowledge is required to use the method correctly. • The probability rate of a low response rate • The possibility of not being able to examine the issue comprehensively.
Press releases and meetings	• Information • Seeking Feedback	• Cheap • Easy to organize • Ability to reach a large number of people	• Difficulty in determining whether the target group has been reached • Difficulty in measuring the success or value of the method • Difficulty in examining the subject in depth • No feedback or very limited feedback
Brain Storm	• Exchanging ideas • Joint decision-making	• Reaching a large number of opinions on a topic • Contribution to a culture of participation • Inexpensive, flexible, easy to organize	• The possibility practical of no results • The possibility of not being able to examine the issue comprehensively.

		possible	
Workshop	• Information • Seeking Feedback • Joint Decision Making	• Ability to generate solution solutions to problems • Inexpensive, flexible, easy to organize being able to, • Ability to examine the subject comprehensively • - Ability to choose specific groups goals • Easier participation thanks to the informal environment	• Not scientific • There may be practical no results • The possibility of a small group dominating the workshop • The probability of obtaining incorrect results with a small and randomly selected group.
Conference	• Information • Seeking Feedback • Joint Decision Making	• Be creative and flexible • Ability for different groups to work together • The possibility of choosing specific goals groups • The subject comprehensively opportunity for examination • The opportunity to discuss different ideas and opinions	• Expensive, time-consuming • The probability of obtaining incorrect results with a small and randomly selected group. • Creating expectations a difference • The likelihood of the results being useful - If not managed well, there is a possibility that a small group could dominate the meeting.
Focus Group • Group discussion led by a moderator		• Faster and less costly than one-on-one interviews • Allows for discussion of different ideas and opinions • - Speeds up the transcription process by facilitating oral discussion	• The possibility of useless information being revealed due to an unsuccessful moderator. • The quality of participants affects data quality.
Search conference	• To form a opinion partnership • Finding solutions to common problems	• Different opportunity to discuss ideas and opinions • Ability to examine a subject in depth • Bringing together experienced decision-makers and knowledgeable individuals	• Potential for undesirable outcomes if not managed properly. • Expensive, time-consuming • Possibility of being dominant a small group conference
Web pages, intranet and e-mail	• Information • Seeking Feedback	• Cheap • Easy to organize • Ability to reach a large number of people • Effective information sharing	• Update requirement • Being contacted by unwanted individuals problem

CHAPTER FIVE

MONITORING

1. INTRODUCTION

Monitoring involves evaluating whether the internal control system is making the expected contribution to achieving the administration's aims and objectives, within the framework of compliance with internal control standards, and identifying actions to address areas for improvement in the system.

Monitoring helps to determine and evaluate whether the administration's activities are carried out in line with the mission and objectives, whether the necessary controls are foreseen within the framework of risk management principles, whether these controls are implemented, and whether communication is open and adequate.

Therefore, monitoring is a process that operates in interaction with other components of the internal control system.

Monitoring is carried out to ensure that the internal control system is functioning as expected and adapting to changes in circumstances, giving management the opportunity to correct control activity problems and control risk before an undesirable event occurs.

Participation is essential in monitoring the internal control system. Monitoring should utilize questionnaires, internal and external audit reports, requests and complaints from individuals and/or administrations, budget information, data related to preliminary financial control, and the opinions of unit managers.

TRACKING Box 1: Why is Tracking Necessary?

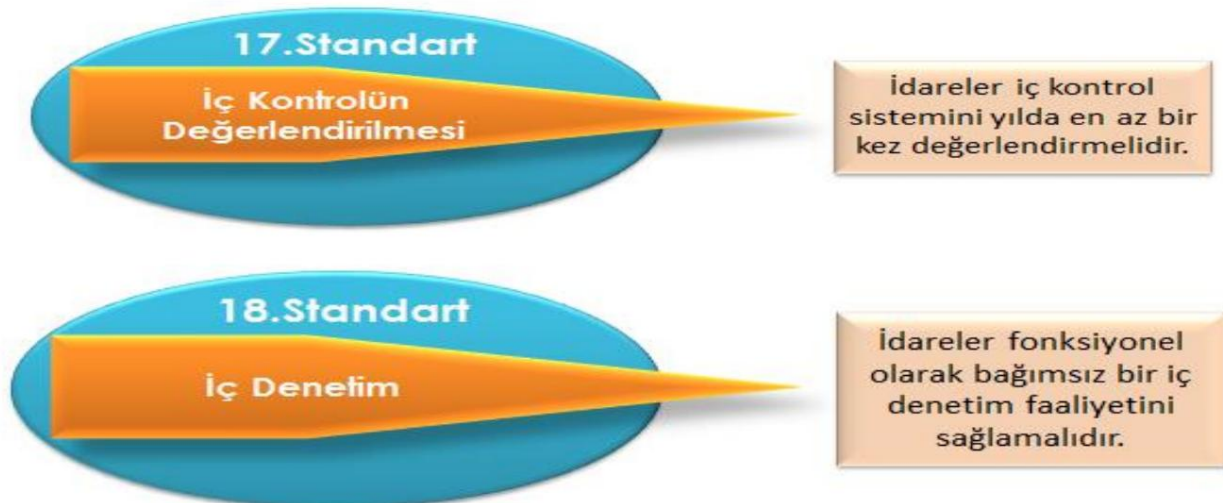
Monitoring is carried out for the following main purposes:

- To identify and resolve problems related to the internal control system in a timely manner,
- To regularly verify the effectiveness of the internal control system,
- To provide evidence for internal control assurance statements.

2. MONITORING STANDARDS

Monitoring encompasses all monitoring activities carried out to assess the quality of the internal control system.

İZ Box 2: Tracking Standards



3. ROLES AND RESPONSIBILITIES

3.1. Monitoring Roles and Responsibilities in Public Administrations

3.1.1. Senior Executive

The primary responsibility for monitoring the internal control system rests with the senior management. Article 11 of Law No. 5018 also emphasizes this point, stating that senior managers are responsible for overseeing and monitoring the functioning of the financial management and control system.

In order for the senior manager responsible for the internal control system to provide assurance, the design and It needs to monitor and evaluate how it works.

The senior executive delegates this responsibility to the internal audit unit, strategy development units (SGB), and expenditure He carries it out through his authorities.

By approving the internal control system evaluation report prepared annually by the senior management. MYK ensures that it is forwarded to MUB.

The senior manager also declares, through the internal control assurance statement, that the management of the internal control system provides reasonable assurance, based on evidence, that the aims and objectives of the system are achieved each year. In this context, they also evaluate the assurance statements included in the unit activity reports submitted by the spending authorities.

The senior manager ensures that the recommendations resulting from internal and external audits are implemented.

On the other hand, information about the compliance studies with the Public Internal Control Standards carried out in the public administrations included in the annexes (1) and (II/B) to the Law No. 5018 is given to the relevant Minister by the senior manager in January of each year.

3.1.2. Internal Audit Unit

The internal audit unit has the function of providing information, making assessments, and making recommendations to management regarding the adequacy, effectiveness, and functioning of the internal control system. It reports these assessments and recommendations to senior management and unit managers within a framework of professional judgment.

The internal audit unit also provides assurance and advisory services to the senior manager, who is responsible for the sound operation of the internal control system. Internal audit reports are submitted directly to the

senior manager. These reports are evaluated by the senior manager and forwarded to the relevant units and the Internal Control Board for necessary action. Internal audit reports and the actions taken based on them are sent by the senior manager to the Internal Audit Coordination Board (IACB) within a maximum of two months from the date the report is submitted. Corrective actions and recommendations suggested by the auditor as a result of the internal audit activity are implemented by the audited unit

within the timeframe specified in the report. The head of the internal audit unit monitors whether the measures specified in the internal audit report have been taken. Internal audit units establish a monitoring system for the implementation of audit reports.

3.1.3. Internal Control Monitoring and Steering Committee (ICMS)

The Internal Control System Evaluation Committee (YKYK) reviews the Internal Control System Evaluation Report (See Appendix 2) prepared by the SGB as a result of the annual evaluation of the internal control system, and after completing any deficiencies in the report, submits it to the senior management for approval with its favorable opinion.

3.1.4. Strategy Development Unit (SDU)

According to Law No. 5018 and related legislation , SGBs (Specialized Control Units) are tasked with conducting studies for the establishment, implementation, and continuous improvement of an internal control system and reporting the results of these studies to the senior management.

Within this scope, SGBs coordinate the evaluation of the internal control system. They conduct this evaluation by forming working groups or using tools such as checklists, surveys, and questionnaires, and present the findings in a report to the senior management with the approval of the Internal Control Management Board.

The SGB manager ensures that the administration's activities are carried out effectively, economically, and efficiently. He/she signs a statement confirming that internal control processes are in place to ensure compliance.

SGB personnel also play an active role in the evaluation process of the internal control system and provide guidance to units in completing the Internal Control System Questionnaire (See Appendix 1) for the evaluation.

3.1.5. Spending Authorities

Spending authorities have a responsibility for continuous monitoring. This includes examining the extent to which controls are implemented in subordinate units and how subordinate unit managers fulfill their monitoring responsibilities within their units.

In addition, spending authorities provide the necessary information to the SGBs for the annual evaluation of the internal control system, complete the Internal Control System Questionnaire (IZ Appendix 1), and sign the internal control assurance statement each year for submission to senior management.

Spending authorities also have the responsibility to take action regarding the recommendations contained in internal and external audit reports.

3.1.6. Other Managers and Employees

Other managers are responsible for the effective functioning of internal controls in their respective areas. Therefore... They are required to monitor all activities and operations within their units.

Because employees are familiar with the organization's daily operations in detail, they can quickly and easily identify problems that arise despite existing control measures. Therefore, it is the responsibility of employees to monitor the internal control system while performing their duties and to inform their manager if they identify a problem.

Employees should also contribute to the evaluation process of the internal control system.

3.2. Other Roles and Responsibilities Related to Monitoring

3.2.1. MYK MUB

Article 55 of the Public Financial Management and Control Law No. 5018 and Article 9 of the Procedures and Principles Regarding Internal Control and Preliminary Financial Control stipulate that standards and methods related to financial management and internal control processes shall be developed and harmonized by the Ministry of Finance, and that guidance services shall be provided to public administrations.

In this context, MYK MUB;

- It monitors whether internal control standards are being complied with.
- Reports from administrations regarding internal control and preliminary financial control regulations and practices.
It monitors the functioning of systems by gathering information.
- By researching national and international best practice examples and implementing them.
He conducts research.

The MYK MUB also annually evaluates the functioning of the internal control system in the public sector, based on the Internal Control System Evaluation Reports submitted and approved by the senior executives of public administrations, and submits its evaluation report to the Senior Executive of the Ministry of Finance and the Minister of Finance. This report is also made public. If the report contains matters related to defense, security, and intelligence, the opinions of the relevant public administrations are sought before making a public statement.

MYK MUB, when deemed necessary, addresses matters included in the reports of public administrations. It can also conduct on-site monitoring activities.

3.2.2. External Audit

External auditing is carried out by the Court of Accounts. The purpose of external auditing is to examine the financial activities, decisions, and transactions of public administrations within the scope of general administration, in terms of their compliance with laws, institutional aims, objectives, and plans, within the framework of accountability, and to report the results to the Turkish Grand National Assembly. External auditing is divided into two types: regularity audits and performance audits. Within the framework of regularity audits, the internal control systems of public administrations are also evaluated, and recommendations are made for their improvement.

4. MONITORING METHODS

The internal control system is monitored through continuous monitoring and specific assessments.

4.1. Continuous monitoring

Continuous monitoring is carried out by personnel performing administrative activities and by managers responsible for hierarchically monitoring them throughout the course of their duties. Continuous monitoring encompasses regular management and oversight activities, comparisons, and other measures taken by personnel while performing their tasks.

Since problems can be identified more quickly and necessary measures can be taken in a timely manner for control deficiencies through continuous monitoring activities, it is recommended that administrations primarily focus on continuous monitoring activities.

Below are some examples of continuous monitoring activities:

• Review and evaluation of financial and activity reports
• Counting company assets and comparing them with accounting records to identify discrepancies. research
• Investigating complaints and allegations from third parties
• Gathering and evaluating employee opinions
• Monitoring employees' compliance with ethical rules
• Holding periodic evaluation meetings
• Evaluation of periodic reports on the achievement of the objectives included in the strategic plan and performance program.
• Evaluation by senior management of monthly reports on financial transactions carried out by spending authorities even though they were deemed inappropriate as a result of preliminary financial control.
• External sources verifying internal processes or uncovering problems. For example, a taxpayer verifying the tax authorities' assessment records by paying their tax debt.
• Implementing the recommendations of internal and external auditors regarding the improvement of the internal control system bringing

4.2. Specific Assessments

Specific assessments are conducted by management and for the purpose of evaluating the effectiveness of the internal control system. These are evaluation activities carried out by employees.

Special assessment activities include conducting self-assessment workshops and questioning. This can be done by using forms/surveys and forming working groups.

Self-assessment workshops contribute to the evaluation of the internal control system, as well as raising awareness among managers and employees about the importance of internal control in achieving management objectives. The workshops are conducted with a facilitator.

Questionnaires/surveys can be used to obtain detailed information about the internal control system. It is advisable to prepare clear and concise questions that do not allow for subjective evaluation, and to design them so that a negative response reveals a potential weakness.

Through questionnaires/surveys, the internal control system can be evaluated as a whole, or only a single component or key process can be assessed (such as Risk Management).

In addition, administrations may request evaluations of their internal control systems from independent external evaluation organizations.

TRACK Box 3: Key Elements of Tracking

- Continuous monitoring and specific evaluation methods are not alternatives to each other, but rather the administration's Both methods should be used, depending on the structure.
- Even if continuous monitoring methods are effectively implemented, the internal control system as a whole It would be appropriate to subject it to a special evaluation.
- When determining the scope and frequency of the specific assessment, consideration should be given to the risk assessment, the competence and experience of the personnel responsible for responding to risks or implementing control activities, and the effectiveness of continuous monitoring methods.
- Deficiencies identified through continuous monitoring and specific assessments should be reported to those in a position to take necessary measures. Procedures for reporting these deficiencies and implementing the relevant corrective actions should also be in place within the administration.
- Monitoring activities are not only carried out in cases of failure, error, mistake, or weakness; they are continuous. and should be carried out in an integrated manner with daily activities, programs and projects.

4.2.1. Evaluation Process

The internal control system is evaluated periodically, and necessary measures are identified. Inclusion in the application is extremely important for ensuring the effectiveness of the system.

The evaluation of the internal control system is a process that includes examining, specifically in terms of internal control components, whether the system provides the expected contribution to achieving the administration's aims and objectives, identifying areas for improvement, and determining corrective measures. Internal control system evaluation should primarily involve active participation from SGBs (Support and Development

Units).



It is recommended that this be done through the Control System Questionnaire (See Appendix 1). The administration may add new questions to the Questionnaire. However, other tools may also be used in the evaluation process.

The evaluation is conducted at least once a year. The evaluation takes place in three-month and six-month periods. It is also possible to do so in that respect.

Coordination of the evaluation process, sending questionnaires to the relevant units, and The task of compiling the responses belongs to SGB's internal control subunit.

A representative from SGB will be assigned to provide support in filling out the questionnaires. A plan should be developed regarding personnel and the evaluation process. The plan should ensure that a representative is assigned to each unit; if the number of personnel is insufficient, at least one responsible staff member should be designated and communicated to the relevant units. This staff member should provide guidance to the units in completing the questionnaires.

The following steps should be followed in the evaluation process of the internal control system.

- First, an opening meeting should be held with the participation of unit managers and SGB representatives. The process for completing the questionnaires should be explained at this meeting.

- The timeline for completing the questionnaire, along with the contact information of the SGB representative, should be submitted to the unit manager along with the questionnaire. Units should be given a reasonable amount of time, no less than one week, to complete the questionnaire.
- When completing the questionnaire, spending units should bear in mind that this process constitutes a self-assessment; in other words, their answers primarily serve to evaluate their own units. Therefore, the functioning of their internal control system should be thoroughly assessed while completing the questionnaire.
- If necessary, assistance should be sought from a SGB representative when filling out the questionnaires.
- When the questionnaire is received by the SGB representative, each question should be checked, and any misunderstandings should be corrected. For this purpose, the SGB representative may discuss the answers in the questionnaire with the unit manager or a person they designate.
- After all questionnaires have been collected, the SGBs should consolidate the questionnaires and prepare an evaluation report using the questionnaire results, primarily, and the following information sources:
 - o Internal and external audit results
 - o Data related to preliminary financial control
 - Other sources of information (opinions of managers, requests from individuals and/or administrations complaints)
- Considering that the evaluation report will be prepared using the above-mentioned information sources (questionnaire, internal and external audit results, preliminary financial control data, etc.), it should also be noted that this process will take time.

Percentage scores should be interpreted separately for each category and for the form as a whole, as shown in Table 1 :

Interpretation of

Internal Control System Questionnaire Results.

% score	Comment
0-25	This indicates that the development of the internal control system is at its lowest level. While there is some awareness, it appears that internal control mechanisms have not yet been implemented within the administration. Urgent guidance and direction are needed to establish an internal control system.
26-50	This indicates a low level of development in the internal control system. It appears that awareness and understanding of the internal control system exist, and efforts have begun to implement internal control mechanisms. However, these efforts need to continue and be implemented more effectively.
51-75	This indicates a moderate level of development in the internal control system. It suggests that internal control mechanisms have begun to be implemented, but need further development. This indicates a high level of development in the
76-90	internal control system. It suggests that the implementation of internal control mechanisms is well-established. It would be appropriate to evaluate what can be done to further improve the implementation.
91-100	This indicates that the internal control system has reached its highest level of development. It shows that the internal control mechanisms are being implemented in the best possible way.

4.2.2. Reporting of Evaluation Results

SGB prepares a report on the activities carried out for the establishment and development of the internal control system, as well as evaluations of the system's operation, effectiveness, and efficiency. (Evaluation)

In preparing the results in the report, the Internal Control System Evaluation Report (See IZ Appendix 2) It would be appropriate to use it.

The "Internal Control System Questionnaire" forms a crucial basis for preparing this report . The report should include information on the functioning of the internal control system, as well as steps taken to strengthen it. Furthermore, the report should address areas where controls are insufficient or inadequate, areas where controls are not functioning properly, areas where controls are excessive, or plans and schedules prepared to address identified problems.

The prepared report is evaluated by the Internal Control System Evaluation Committee (ICSE), and after any deficiencies in the report are corrected, it is submitted to the senior management for approval with a favorable opinion.

The internal control system evaluation report approved by the senior management must be forwarded by the Internal Control Board (ICB) to the Central Executive Board (CMB) by the end of June of the following year.

4.2.3. Monitoring of Evaluation Reports

The measures, activities, and regulations to be taken regarding the areas identified as open to improvement in the Internal Control System Evaluation Report should be determined within the framework of management responsibility. Unit managers will need to take action to address gaps in some areas.

Furthermore, if horizontal problems are identified where most units receive poor grades, it would be appropriate for senior management to initiate actions to improve the situation.

The necessary measures, activities, and regulations should be implemented within the framework of an action plan and linked to a specific timeframe. The SGB (Sectoral and Technical Committee) should monitor and evaluate the results of the implementation of these measures, activities, and regulations at least every six months and inform the senior management about the results.



5. ACTIONS TO BE TAKEN BY THE MINISTRY OF HEALTH REGULATIONS REGARDING INTERNAL AUDIT REPORTS

Article 64 of Law No. 5018 states that reports submitted to the senior manager by internal auditors shall be evaluated by the senior manager and sent to the relevant units and the SGB (Self-Employment and Control Board) for necessary action. Within this framework, SGBs may perform the following actions based on these reports sent by the senior manager:

• Identifying training needs for the administration based on identified deficiencies in internal control and taking initiatives to organize training programs.
• Taking into account internal audit findings, the leadership is working towards improving the internal control system. Making suggestions to the manager.
• Necessary records and follow-up regarding public losses identified in internal audit reports. execution of operations.
• Making internal adjustments to address the discrepancies in practices revealed by internal audit reports.

MONITORING SECTION ATTACHMENTS

APPENDIX 1. Sample Internal Control System Questionnaire

INTERNAL CONTROL SYSTEM QUESTIONNAIRE

This questionnaire is designed to evaluate the internal control system. It will also help determine the extent to which the internal control system facilitates the achievement of objectives in the context of changing conditions, resources, and risks. Realistic answers from respondents are of great importance and will be used to determine the level of sophistication of the internal control system within the administration.

Unit managers are responsible for completing this questionnaire after thoroughly evaluating the functioning of the internal control system within their respective units. In this context, unit managers will send the completed questionnaire, under the guidance of the Internal Control Boards (ICBs), to the ICBs. The ICBs will then prepare a report using this questionnaire and, after obtaining approval from the senior management, will submit it to the Central Executive Board (MYK MUB).

Completing the Questionnaire

This questionnaire is based on the components of internal control and has **five sections** :

- | |
|---------------------------------|
| • Control Environment |
| • Risk Assessment |
| • Control Activities |
| • Information and Communication |
| • Monitoring |

Each section contains questions regarding the functioning of the internal control system within the framework of the components mentioned above. Care should be taken to ensure that the answers given in the questionnaire are consistent with the administrative action plans prepared for compliance with the Public Internal Control Standards.

The answer section of the questionnaire consists of three options: YES, NO, and UNDER DEVELOPMENT. There is also a fourth column for EXPLANATION. **YES** means that the topics mentioned in the question are understood and implemented as required within the unit. **NO** means that these topics are not understood and implemented throughout the unit. **UNDER DEVELOPMENT** means that the topics mentioned in the question are partially understood and implemented in some parts of the unit. **The EXPLANATION** section should include any evidence and interpretations. The questions are followed by guidance to help better understand the question. In the evaluation of the questionnaire, the point value of each answer will be used. A YES answer will be worth 2 points, an UNDER DEVELOPMENT answer will be worth 1 point, and a NO answer will be worth 0 points. A

separate total score will be calculated for each section of the questionnaire, as well as a general total score for the entire questionnaire.

• If the answer to a question is NO, the unit manager should be responsible for developing the relevant areas. Action must be taken by them.

• If a question is answered with "UNDER DEVELOPMENT," the unit manager should evaluate what can be done to make progress in that area.

• If the answer to a question is YES, it means there are no areas that need improvement in that area. Please be mindful that this questionnaire is a self-

assessment and that the internal control system is a new practice for public administrations, so please provide realistic and honest answers.

• If you have any doubts while filling out this questionnaire, please contact SGB. your application.

No	Questions				Explanation
	Point	2	0	1	
	CONTROL ENVIRONMENT				
CONTROL ENVIRONMENT: The control environment provides a general framework that forms the basis for other elements of the internal control system. It is a concept used to define the mission, communicate it to the organization's personnel, and create an organizational structure and corporate culture that is consistent with these. Key elements influencing the control environment include personal and professional integrity, ethical values of management and personnel, a supportive attitude towards internal control, written rules and practices for human resources management, organizational structure, management philosophy, and business practices. Detailed explanations can be found in the Control Environment section of the Public Internal Control Guide. Please read the relevant section before answering the following questions.					
1	In your unit, Public Internal Affairs Control Are the standards known? <i>(There will be training sessions and meetings organized to raise awareness on this issue.)</i> <i>suitable</i>				
2	Are there any initiatives within your unit to increase awareness and ownership among managers and staff regarding the internal control system and its functioning? For example, are activities such as holding periodic information meetings on internal control, preparing promotional brochures, including internal control in in-service training programs, and making information and documents related to internal control easily accessible on the unit's website/intranet?				
3	Are managers and staff at all levels within your unit informed about ethical conduct principles and their responsibilities regarding these principles? For example, guidance given towards internalizing public ethics rules.				

³ If the "Yes" option is selected, evidence (internal regulations, details of activities performed, etc.) should be included in the "Description" section.

⁴ If the "No" option is selected, the necessary explanations must be included in the "Description" section.

⁵ If the "Under Development" option is selected, the necessary explanations (details of planned activities, etc.) should be provided in the "Description" section.

	Are managers and staff members encouraged to participate in training sessions and organized meetings? <i>(It would be appropriate to include ethical conduct principles in the basic, preparatory, and in-service training programs organized and implemented for your unit's personnel.)</i>				
4	Are managers and staff at all levels within your unit informed about the sanctions that will be applied in cases of unethical behavior? <i>(If the answer to this question is "yes," then how this awareness was achieved should be explained.)</i>				
5	Has your unit developed a standard regarding the timing and methods for services provided directly to citizens? <i>(In answering this question, the studies conducted within the scope of the Regulation on the Principles And Regarding the Procedures to be Followed in the Provision of Public Services should also be considered.) assessable.)</i>				
6	Is access provided to all outputs related to your unit's work and processes by personnel and relevant authorities?				
7	Does your unit have appropriate mechanisms (surveys, face-to-face interviews, meetings, electronic applications, etc.) through which staff and those receiving services from the unit can report their evaluations, suggestions, and problems? Are they being used effectively? <i>is that right? (If applicable, what methods are used?) Please provide brief information about it.</i> <i>Confidentiality of the surveys to be conducted It is recommended that it be thorough.</i>				
8	Has your unit's mission been defined and announced in writing? <i>(The mission statement can be announced to staff via bulletin boards, the intranet, and email.)</i>				
9	A job description for your unit and subunits Is there a regulation (guideline, circular, approval, etc.)? <i>(If the answer to this question is "No," then these procedures will be ^{What} ^{time} carried out.) as planned</i>				

	<i>(It should be noted.)</i>				
10	Are job descriptions clearly defined in writing for managers and staff at all levels within your unit? Have these been communicated to the relevant managers and staff? <i>(Personnel job descriptions should be prepared based on the job description of the unit in which the personnel work, communicated to the relevant personnel, and reviewed and updated at least once a year.)</i> <i>When answering this question, it should also be assessed whether there are internal regulations in place for defining and periodically updating the format and content of personnel job descriptions.</i>				
11	Does your unit's organizational chart show the division of labor and appropriate reporting channels for accountability?				
12	Are the responsibilities of your unit and subunits aligned with the mission of your administration and unit? <i>(The unit and its subunits must ensure that their tasks are aligned with the mission, and the organizational structure and tasks must be revised in line with these changes through continuous monitoring.)</i>				
13	Have sensitive tasks and related procedures been identified within your unit? <i>(It is recommended that these procedures be defined in writing, communicated to personnel, and that appropriate control activities (separation of duties, rotation, designation of backup personnel, etc.) be determined for sensitive tasks.)</i>				
14	Have mechanisms been established within your unit to allow managers at all levels to monitor the results of assigned tasks? <i>(If the answer is "Yes," then the mechanisms in place (reports, work plans, periodic meetings, automation program, etc.) should be specified.)</i>				

15	In a writtenly defined role Are there promotion procedures? <i>(These procedures should be determined taking into account the performance of the personnel, and the personnel should be informed about these procedures.)</i>				
16	Is the unit determining the necessary training needs for each task, and are training activities to address these needs planned and implemented annually?				
17	Your unit Do managers share their evaluations of staff competence and performance with the relevant staff members? <i>(It is recommended that managers share the results of employee performance evaluations with their employees.)</i>				
18	Are measures taken in your unit to improve the performance of personnel whose performance is deemed insufficient according to performance evaluations? <i>(For example, are measures such as providing training to improve the performance of</i> <i>personnel deemed insufficient, holding meetings about their areas of weakness to motivate them, or assigning them to duties under the supervision of experienced personnel?)</i>				
19	In your unit Are there any reward mechanisms developed and implemented for high-performing personnel? <i>(Reward/ motivation mechanisms for high-performing personnel (by the manager)</i> <i>(It is recommended that criteria such as recognition in the presence of employees, certificates of achievement, access to domestic and international career development opportunities, etc., be developed and communicated to all personnel.)</i>				
20	Does your unit have human resources procedures in place for its personnel (recruitment, transfers, promotions, performance evaluations, etc.)?				
21	Signatures in workflow processes within your unit				

	And have the approval authorities been determined? <i>(It is recommended that the workflow processes be defined and the signing and approval authorities for these processes be determined and announced.)</i>				
22	Delegations of authority to be made within your unit Have the principles been defined in writing? <i>(The scope, amount, duration, and whether the delegated authority can be further delegated to someone else must be included in the delegation of authority. Furthermore, care must be taken to maintain a balance between authority and responsibility during the delegation process.)</i>				
23	In your unit Have to be transferred the minimum requirements (knowledge, skills, and experience) for authorized personnel been determined?				
24	In your unit transferred authority of personnel, regarding the use of authority Is there any regulation requiring the delegate to report to the delegator at certain intervals?				
TOTAL SCORE - CONTROL ENVIRONMENT					
RISK ASSESSMENT					
RISK ASSESSMENT: Risk assessment is the process of identifying, analyzing, and determining necessary measures to mitigate risks that could hinder the achievement of the administration's objectives. In this section, the administration should conduct a self-assessment of its risk perception and capacity to cope with risks through the following questions. Detailed explanations can be found in the Risk Assessment section of the Public Internal Control Guide. Please read the relevant section before answering the following questions.					
1	Has a reporting procedure been established for monitoring and evaluating the level of achievement of the targets included in the performance program? <i>If the answer is "yes," then a brief explanation of how the monitoring and evaluation process works in practice should be provided.</i>				
2	Are there procedures in place to ensure alignment with strategic plans and performance programs during the budget preparation process? <i>(The activities and projects through which the aims and objectives shown in the strategic plan will be achieved, the indicators to be monitored, and the resource requirements for these activities and projects are shown in the performance programs. Therefore, units should take these plans and programs into account when preparing their budget proposals.)</i>				

	<i>(They need to take this into consideration.)</i>				
3	Is there a procedure in place to ensure that the activities carried out within your unit are aligned with the aims and objectives defined in the strategic plan and performance program? <i>(In terms of the effective, economical, and efficient use of resources, units should focus their activities on the aims and objectives stated in the administration's strategic plan and performance program.)</i>				
4	Has your unit defined specific objectives within your area of responsibility that align with the administration's goals?				
5	Has the risk strategy document, approved by senior management, been communicated to all employees in your unit?				
6	Are the tasks and responsibilities related to risk management in your unit clearly defined and documented in writing? <i>(Clearly defining roles and responsibilities in risk management and Assigning these tasks and responsibilities to appropriate, competent, and authorized individuals creates a strong foundation for risk management. If a Risk Strategy Document has been prepared for your administration, it should also include tasks and responsibilities related to risk management. And</i>				
7	Are risks identified within your unit at the unit/program and sub-unit/operational level?				
8	Are the risks identified in your unit being assessed, along with their potential impacts and probability of occurrence? <i>(Probability and impact of identified risks)</i> <i>(It must be measured and shown in numbers.)</i>				
9	Are the risks identified in your unit prioritized according to risk scores (Impact x Probability) or severity levels? <i>Prioritizing risks according to their severity ensures efficiency in resource allocation.</i>				

10	The risks identified in your unit are appropriate. Are the vehicles being recorded? <i>(Recording risks helps to create evidence for decisions made, and allows individuals to see and monitor their responsibilities within risk management.)</i> <i>If the answer to this question is "Yes," then the tools used for recording risks (risk report form, software, etc.) should be specified.</i>				
11	When determining the response method to the risks identified in your unit, is a cost-benefit analysis conducted? <i>(When determining responses to risks, care must be taken to ensure that the benefit of the response outweighs the cost.)</i>				
12	Is the probability or impact of identified risks within your unit reviewed periodically to determine if there have been any changes or if new risks have emerged? <i>(Identified risks should be reviewed at least once a year according to their severity.)</i>				
13	Personnel in the risk management process Is a contribution being received? <i>(Personnel taking ownership of the risk management process and viewing it as part of their work will increase the effectiveness of a strong corporate risk management process against risks.)</i> <i>If you answered "yes" to this question Please explain how you made this contribution.</i>				
14	Are the managers and staff in your unit aware of their responsibilities regarding risk management? And <i>(When answering this question, the methods used to inform and raise awareness among And personnel regarding their responsibilities in risk management should be evaluated, and the tools employed in this context should be explained.)</i>				
15	If your unit has risks that need to be managed jointly with other units, those risks... subject				

	Is the necessary cooperation and communication being maintained with the relevant unit regarding its management?				
16	Are the experiences gained from risk management within your unit shared with other units? <i>(Particularly regarding newly emerged risks and methods of dealing with them, both positive and negative)</i> <i>Sharing experiences and knowing what can go wrong in this context can prevent mistakes from being repeated and help in dealing with risks.</i> <i>It will increase the effectiveness.</i> <i>If you answered "yes" to this question, please explain how experiences were shared (such as working meetings, practical training, sharing information through different communication channels, sharing best practices, negative examples or mistakes).</i> <i>sharing,</i>				
TOTAL SCORE - RISK ASSESSMENT					
	CONTROL ACTIVITIES				
CONTROL ACTIVITIES: Control activities are policies and procedures established to ensure the achievement of objectives and to manage identified risks. Detailed explanations can be found in the Control Activities section of the Public Internal Control Guide. Please read the relevant section before answering the following questions.					
1	Are effective control strategies and methods defined and implemented for each activity and risk within your unit? <i>(Established controls should be compatible with the risks, and different control methods should be determined according to the nature of the risk.)</i> <i>Control strategies and methods should be defined and implemented as follows: regular review, sampling control, verification, reporting, coordination, authentication, analysis, authorization, supervision, inspection, monitoring, periodic inspection and security of assets, etc.</i> <i>(Controls within the unit should include pre-process control, process control, and post-process control, where necessary.)</i>				
2	A cost-benefit analysis is conducted when identifying control activities in your unit.				

	Really? <i>(The cost of the control method determined in the unit should be compared with its expected benefit, controls whose cost outweighs their benefit should be identified, and less costly alternative controls should be selected.)</i>				
3	In your unit Are the control effectiveness of the implemented activities regularly reviewed? <i>(The effectiveness and functioning of control activities should be monitored to ensure they are carried out as planned. Necessary evidence regarding the functioning of controls should be collected and analyzed periodically.)</i>				
4	4 Your unit's activities and financial decisions and Are there any existing written procedures transactions related to this? <i>(Your unit must have written procedures regarding its activities and financial decisions and transactions. These procedures and related documents should cover the initiation, implementation, and completion phases of the activity or financial decision and transaction. The procedures and related documents must be current, comprehensive, compliant with legislation, and understandable and accessible to relevant personnel.)</i>				
5	5 Your unit Are the necessary checks being carried out by managers to ensure that the procedures are implemented effectively and consistently? <i>(The unit's activities and operations must be carried out within the framework of the regulations established in this field.)</i> <i>Compliance with these regulations must be systematically checked by managers. For this purpose, control processes such as initials, approvals, checklists, and physical counts can be defined. In this context, managers should monitor whether the work performed by personnel complies with the regulations. Managerial instructions should be created regarding how any identified errors or irregularities will be rectified.</i> And What				

6	6 Separation of duties within your unit principle Is it being implemented? Explain in which situations you apply the principle of separation of duties. <i>(The tasks of approving, implementing, recording, and controlling each activity or financial decision and transaction should be assigned to different individuals and supported by written documents that uphold the principle of separation of duties.)</i> <i>In cases where the principle of separation of duties cannot be fully implemented due to insufficient personnel, managers must be aware of the risks and take necessary precautions. In such situations, alternative control procedures should be established to manage the risk.</i>				
7	7 Are measures taken in your unit to address factors affecting the continuity of operations, such as staff shortages, temporary or permanent departures, transitions to new information systems, changes in methods or regulations, and extraordinary circumstances ? <i>When the answer is "yes," it relates to this. Evidence can be presented.</i>				
8	8 Is the proxy system effective in your unit? Is it being implemented in this way? <i>(Substitute personnel should be appointed in accordance with the proper procedures when necessary.) Personnel appointed as acting personnel must possess the necessary qualifications. Detailed internal regulations should be established regarding the institution of acting as a substitute, as stipulated in personnel laws, and the qualifications required of substitute personnel should be defined in detail.</i>				
9	In your unit Do departing personnel report to newly assigned personnel on the status of the work and procedures they carried out? <i>(Managers should ensure that personnel leaving their positions prepare a report detailing the status of their work or tasks and providing it to newly assigned personnel. The report should include a list of important ongoing tasks, priority risks, and deadlines.)</i>				

	(A list of tasks and similar matters should be included.)				
10	¹ Does your unit have mechanisms in place to ensure the security of the information systems used? <i>(When answering this question, it should be assessed whether the administration has an information security management system, ISO certification regarding information security, etc.)</i>				
11	Have authorizations been granted within your unit for data and information entry into the information system and for access to it? <i>(Access to the information system should only be granted to authorized personnel. For this purpose, continuously updated information security software should be used to access computer programs.)</i> <i>When working with documents, regulations regarding the protection of the specified level of confidentiality must be observed.</i>				
12	Does the information system have an adequate backup mechanism and tested emergency plans/action plans in place? repair				
TOTAL SCORE - CONTROL ACTIVITIES					
	INFORMATION AND COMMUNICATION				
INFORMATION AND COMMUNICATION: Information and communication encompasses an appropriate information, communication, and record-keeping system that ensures necessary information is transmitted to those who need it—personnel and managers—in a specific format and within a timeframe that allows stakeholders to fulfill their responsibilities regarding the achievement of objectives and internal control. Detailed explanations can be found in the Information and Communication Section of the Public Internal Control Guide. Please read the relevant section before answering the following questions.					
1	¹ Does your unit have an effective internal communication system in place, encompassing both horizontal and vertical communication, whether written, electronic, or verbal? <i>(When answering the question, the methods/tools by which staff members communicate with each other and with their managers should be identified and evaluated to determine whether they are appropriate and/or effective.)</i> <i>(Employees should be in contact with managers at all levels, including senior management, to ensure they receive the information necessary to perform their duties without interruption.)</i>				

2	2 Does your unit have an external communication system in place to ensure effective communication with external stakeholders?				
3	3 Do the current internal and external communication systems allow staff and/or external stakeholders to convey their expectations and complaints? <i>(For example, it should be evaluated whether the Law No. 4982 on the Right to Information is effectively implemented within the institution, whether requests and complaints are answered in a timely manner, and whether there is a system in place that allows employees to submit their complaints and suggestions to the management.)</i>				
4	4 In your unit, are the duties and responsibilities of the personnel, as well as what is expected of them within the scope of the unit's mission and objectives, defined in writing by the managers and communicated to the relevant personnel? <i>(Managers at all levels should communicate their expectations to personnel within the scope of the unit's mission and objectives, and within the scope of their duties and responsibilities.)</i>				
5	5 Do the current information systems allow for the monitoring of objectives set by the administration/unit and for effective oversight and evaluation of activities carried out in line with these objectives? And <i>(The management information system should be designed to generate the information and reports that managers need in decision-making processes and to provide the opportunity to perform analysis.)</i>				
6	6 In your unit, has it been clearly defined and communicated to personnel which reports will be prepared, by whom, how often, when they will be submitted, what their basis will be, and who will review the prepared reports? <i>(Horizontal and vertical reporting networks should be established in writing within the unit, and sub-units and personnel should be informed about the reports that need to be prepared regarding their duties and activities.)</i>				
7	7 Recording, classifying, preserving, and providing access to the unit's work and transactions.				

	Is there an archive and documentation system in place that complies with the specified standards?				
8	8 Does your unit have a comprehensive and up-to-date record-keeping and filing system in place for recording and classifying all incoming and outgoing documents – including electronic ones – as well as internal communications, work, and transactions? <i>(The record-keeping and filing system must be comprehensive, up-to-date, and conform to established standards; it must also be accessible and traceable by managers and staff.)</i> <i>When answering this question, it should also be evaluated whether the provisions specified in the Prime Ministry Standard File Plan Circular (2005/7) and the Electronic Document Standards Circular (2008/16) have been complied with.</i>				
9	9 Is your unit's staff aware of the procedures for handling reports and complaints from both within and outside the administration? <i>(Reporting procedures should be announced via bulletin boards, internet/intranet pages, and similar methods.)</i>				
10	Does the whistleblowing system include appropriate tools for reporting potential or ongoing irregularities, corruption, and problems from within and outside the organization? <i>(Employees and external stakeholders should be adequately informed about these tools.)</i>				
11	Does the whistleblowing system include <i>procedures</i> to ensure the safety of personnel making reports (such as preventing unfair or discriminatory treatment) ? <i>(Managers should take necessary measures to ensure that personnel who report incidents are not subjected to unfair or discriminatory treatment.)</i>				
TOTAL SCORE - KNOWLEDGE AND COMMUNICATION					
	MONITORING				
MONITORING: The internal control system is a dynamic process that must continuously adapt to the risks and changes faced by administrations. Therefore, the internal control system needs to be monitored to ensure it adapts appropriately to changing objectives, the environment, resources, and risks. Effective and...					

Effective monitoring is based on the design and implementation of monitoring procedures that are relevant to the administration's objectives, meaningful, and that assess important controls related to risks.

When properly designed and implemented, monitoring provides administrations with accurate and convincing information about the effectiveness of the internal control system, identifies internal control deficiencies in a timely manner, and communicates them to those who will take corrective action and, if necessary, to senior management. In this way, deficiencies encountered in the control process are corrected before they significantly harm the administration's objectives.

Detailed explanations can be found in the Monitoring Section of the Public Internal Control Guide, and the following questions should be answered. Please read the relevant section before answering.

1	Is internal control effective in your unit? Are meetings being held to allow managers to provide feedback on whether the process is working or not?				
2	2 Are continuous monitoring activities effectively implemented in your unit? (It is recommended that administrations <i>prioritize</i> continuous monitoring activities, such as <i>reviewing and evaluating financial and activity reports, investigating complaints and allegations from third parties, etc., as these activities</i> allow for quicker identification of problems and timely measures to address control deficiencies .)				
3	3 Is your unit's internal control system evaluated at least once a year? (Please provide information on the frequency of evaluation of the internal control system in your unit and the methods used.) The internal control system should be monitored on a continuous basis and evaluated using specific assessment methods when necessary. (The internal control system can be evaluated through the creation of a study or by administering a questionnaire.) special group form				
4	4 In evaluating internal control, are the opinions of managers, requests and complaints from individuals and/or institutions, and reports prepared as a result of internal and external audits taken into consideration?				
5	5 Your unit Is there And effective collaboration between management staff and the internal audit unit? (What has been done to increase the awareness level of your unit's managers and staff regarding internal audit activities?)				

	(Write briefly.)				
6	6 Drink control Based on the assessment results, are the necessary measures identified and implemented? <i>(Please briefly describe the person and unit responsible for monitoring the measures within your unit, and the monitoring method. To which management level and at what intervals are the monitoring results shared? Please specify.)</i>				
7	6 Are the action plans prepared regarding the measures to be taken based on internal audit reports being followed in your unit? <i>(If your answer is "yes," please provide information about the monitoring method used.)</i>				
TOTAL SCORE – VIEWERSHIP					
TOTAL:					

IZ APPENDIX 2. Internal Control System Evaluation Report

.....(NAME OF THE ADMINISTRATION WILL BE WRITTEN HERE) INTERNAL CONTROL SYSTEM EVALUATION REPORT YEAR.....	
CONTENTS	
I. INTRODUCTION	
A. Mission and Vision	
<i>Public administrations preparing strategic plans should include the mission and vision statements of the strategic plan in this section.</i> <i>Public administrations that are not required to prepare a strategic plan may include their mission and vision statements in this section if they have already defined them.</i>	
B. Organizational Structure	
<i>This section should address the organizational structure of the administration.</i>	
II. INTERNAL CONTROL SYSTEM QUESTIONNAIRE RESULTS	
<i>The questionnaire results should be interpreted, and this section should include summary information on the strengths and areas for improvement of each internal control component, broken down by unit.</i>	
II.1. Control Environment	
II.2. Risk Assessment	
II.3. Control Activities	
II.4. Information and Communication	
II.5. Monitoring	
III. OTHER INFORMATION	
<i>The following section should include data obtained from the recommended information sources for evaluating the internal control system.</i>	
III.1. Internal Audit Results	<i>The evaluation should explain how the results of the internal audit were used.</i>
III.2. External Audit Results	<i>If an external audit has been conducted by the Court of Accounts, the evaluation should explain how the results of the external audit were interpreted.</i>

III.3. Other Information Sources	<i>If data relating to preliminary financial control, requests and complaints from individuals and/or administrations, and other information were used in the evaluation, this should be explained below.</i>
Data Relating to Preliminary Financial Control	<i>If there are internal regulations regarding prior financial control, these regulations should be evaluated. This section should also include a consolidated summary of the financial decisions and transactions subject to preliminary financial control during the year, broken down by type and amount, as well as approved and disapproved financial decisions and transactions carried out by spending units despite being disapproved.</i>
Requests and Complaints from Individuals and/or Administrations	<i>This section should describe how requests and complaints from individuals and/or administrations are used in evaluating the internal control system and the results obtained.</i>
Other Information	<i>If any information other than that described above has been used, it should be included in this section.</i>
IV. DEVELOPMENT OF THE INTERNAL CONTROL SYSTEM	
<i>This section should explain the progress/regression recorded in the internal control system since the previous Internal Control System Evaluation Report, along with the reasons for it.</i>	
V. CONCLUSION AND RECOMMENDATIONS	
<i>Based on an evaluation using external and internal audit reports, questionnaires, and other information sources, this section should highlight the strengths and areas for improvement in the administration's internal control system, as well as the steps that need to be taken to strengthen these areas.</i>	
V.1. Strengths	
V.2. Open to Improvement Areas	
V.3. Recommendations for Action	

CONTRIBUTORS TO THE PREPARATION OF THE PUBLIC INTERNAL CONTROL GUIDE

INSTITUTION-NAME/SURNAME
UK AUDIT OFFICE
Janet Thomas
Jo HOWEY
Bob Shambler
Gurdip BHAMBRA
Susan Swingle
John Powell
Malcolm McCarthy
MINISTRY OF FINANCE (GENERAL DIRECTORATE OF BUDGET AND FINANCIAL CONTROL)
Mehmet BÜLBÜL, İafak
Birol ACAR, Kamile ÖZEL,
Ayşegül MUTLU,
Fulya TÜRKEN, Mert
ÇETİNKAYA, Umut
KORKMAZ, Sibel YILMAZ,
Gamze Yüdem SÜLER,
Ergun UNUTMAZ,
Nihal SALTİK TURAN, Esma
Meltem KILIÇ, Barış
TATLISOY, Pınar BAŞPINAR,
MINISTRY OF FINANCE
(STRATEGY
DEVELOPMENT
DEPARTMENT)
İyılca ARSLAN,
Bülent BOZBAŞ, Ayşe
KAYMAK, PRIME
MINISTRY , Mustafa
DöR, Zübeyde
ÇINAR, İlker ERALP,
Osman
KOCAMAN, Uğur AKARSU,
UNDERSECRETARIAT
OF TREASURY, Onur ATAÖYÜ,
Kamil KILINÇ, Sevil
ÇATAK, Rabia
CANBOLAT,
Mücahit DUMAN, Mustafa
Gülbüz TURGUT,
MINISTRY OF DEVELOPMENT, İrfan
HALICI, Ali KARAGÖZ, Ömer Faruk
GÜLSOY, Ercan
SALKIM,
GENDARMERIE GENERAL
COMMAND, A.
Tayyar ERAY

