Journal of Engineering and Technology
DergiPark
AKADEMİK

Journal of Engineering and Technology 5;1 (2024) 11-21

ISO 27001, KVKK, and GDPR: A Comparison of Information Security and Data Protection Standards

[a]Melis Böke Yazıcıoğlu

[a,c]Iskenderun Technical University, Faculty of Engineering and Natural Sciences, Department of Computer Engineering, 2017, HATAY/TURKEY

[a] bokemelis@gmail.com

ARTICLE INFO

Article history:
Received May 11, 2024
Received June 15, 2024
Accepted June 28, 2024
Available online June 29, 2024

Key words:
Information Security
KVKK
GDPR
Data Protection
ISO 27001

* Corresponding author.
E-mail address:
bokemelis@gmail.com

ABSTRACT

In today's digital age, safeguarding information security and data protection is crucial amid increasing cyber threats. ISO 27001:2022 focuses on establishing and executing an organization's information security management system, emphasizing risk management, and safeguarding information assets. On the other hand, GDPR and KVKK serve as legal frameworks governing the protection and processing of personal data. This article offers a detailed exploration of these standards, delineating their benefits, requirements, and the intricate landscape of compliance challenges businesses may face. By providing practical insights, it aims to furnish a vital framework for addressing information security and data protection concerns and empowering businesses to navigate these realms effectively.

1. Introduction

Information security and data protection are among the most crucial and complex issues of today's digital age. With the rapid advancement of technology and the widespread digitization, access to information increases, while cyber threats and data breaches also continue to rise. This situation poses a significant concern for both individuals and organizations. To address these concerns and ensure the security of data, international standards and local regulations have become increasingly important. In this context, standards and regulations such as ISO 27001:2022, GDPR (General Data Protection Regulation), and KVKK (Personal Data Protection Law) come into play. In this study, ISO 27001, GDPR, and KVKK standards will be examined in detail, and the benefits and requirements they provide to businesses will be thoroughly discussed. Additionally, a comparison of these standards in terms of security and compliance for businesses will be conducted, and the scope and requirements of each will be examined in detail. Finally, the process of compliance with these standards and the difficulties that businesses may encounter in this process will be addressed, such as resource constraints, enhancing technical infrastructure, and adapting to cultural shifts, along with practical recommendations. In this way, an important framework for information security and data protection will be provided, assisting businesses in operating more effectively in these areas.

2. ISO 27001: Information Security Management System

ISO 27001 is an international standard that guides an organization in establishing, implementing, monitoring, reviewing, and continuously improving its Information Security Management System (ISMS). This standard standardizes the process of managing information security by providing best practices necessary for organizations to protect their information assets. The Information Security Management System (ISMS) Standard covers all types of organizations (e.g., commercial enterprises, governmental agencies, non-profit organizations) [1]. There are main components of ISMS within the framework of ISO 27001.

2.1 Establishment and Implementation of ISMS

ISO 27001 requires an organization to establish its information security policy, define information security objectives, and establish the necessary processes and procedures to achieve these objectives. The information security policy mandated by ISO 27001 sets out an organization's information security objectives and commitments. The information security policy forms the foundation of an organization's information security culture. Effective implementation of the ISMS also involves raising awareness among all employees about information security and encouraging their active participation, thereby fostering the creation of an information security culture and ensuring that commitments are embraced by all employees. This enhances the organization's ability to protect its information assets and become more resilient against cyber threats.

Risks and Threats:

- **Information Security Breaches**: Failure to implement information security policies without necessary precautions may lead to risks such as information security breaches and data leaks.
- **Internal and External Threats**: Malicious individuals or groups from within or outside the organization may damage or gain unauthorized access to information assets. This could manifest as unauthorized access, ransomware attacks, or other cyber threats.
- **Legal and Regulatory Compliance Issues**: Non-compliance with standards like ISO 27001 can expose organizations to legal and regulatory issues, including fines, reputational damage, and other legal consequences.
- **Business Continuity and Operational Risks**: Information security breaches or cyberattacks can affect business continuity and create operational risks, such as data loss or service disruptions.

2.1.1. Risk Management

The ISO 27001 Standard enables organizations to identify, analyze, and evaluate risks that threaten the security of their information assets. Appropriate controls must be implemented to reduce these risks to an acceptable level. The Risk Management process consists of steps such as identifying risks, analyzing risks, evaluating risks, determining control measures, and assessing the acceptability of risks. Risk analysis activities are conducted within the defined scope of the ISMS. The scope of the ISMS also encompasses the scope of risk analysis [2].

2.1.2. Implementation of Controls

ISO 27001 provides a set of control measures and recommends organizations to implement these controls within the scope of their Information Security Management System (ISMS). These controls encompass the security measures necessary for organizations to protect their information assets, enhance resilience against cyber threats, and ensure compliance with legal regulations. The control measures offered by ISO 27001 assist organizations in reducing information security risks and safeguarding their information assets. These controls can be adapted and implemented to meet the specific needs of organizations and industry requirements.

2.1.3. Information Security Policy

When organizations begin their efforts to ensure information security, they should first establish and document rules for all types of information security activities. Written rules are necessary for the planning, implementation, and continuous improvement stages of activities aimed at ensuring information security. In this regard, various guiding documents such as policies, procedures, guidelines, and instructions can be prepared. The foundation of these documents is the information security policy [3]. An organization must establish and implement an information security policy because this policy provides a framework for protecting the organization's information assets and building resilience against cyber threats. This policy defines the organization's information security objectives, responsibilities, and management approach. Establishing and implementing the organization's information security policy is a critical step in creating and maintaining an information security culture.

2.1.4. Continuous Improvement

The principle of continuous improvement in ISO 27001 is an important component for enhancing the effectiveness and efficiency of an organization's Information Security Management System (ISMS). This principle involves regularly reviewing and improving processes and controls. The continuous improvement principle of ISO 27001 enables organizations to continually enhance their information security performance.

3. Personal Data Protection Law (KVKK) and General Data Protection Regulation (GDPR)

Personal Data Protection Law (KVKK):

The Personal Data Protection Law (KVKK) is a regulation enacted in Turkey, which came into effect on April 7, 2016. It encompasses provisions regarding the processing, protection, and lawful utilization of personal data. The primary objective of the KVKK is to safeguard the privacy and security of individuals' personal data, ensure the lawful processing of such data, and protect the rights and freedoms related to personal data.

Data processing rules can be listed as follows [4]:

- Must comply with the legal system in Turkey and align with principles of fairness,
- Data should be verifiable and up-to-date when needed,
- Data processed should be limited, relevant to the purpose for which it is processed, and retained for the necessary duration.

General Data Protection Regulation (GDPR):

The General Data Protection Regulation (GDPR) is a comprehensive regulation concerning the processing and protection of personal data within the European Union (EU). It came into effect on May 25, 2018, and affects all organizations and individuals located within and outside the EU.

- Data processing must be transparent and compliant with the law.
- Data should be limited to the purpose for which it is related.

- Data quality, accuracy, and accountability should be ensured.
- Time constraints should be applied to the retention of relevant data.
- The confidentiality and integrity of the data must be maintained [5].

When these two laws are compared with each other, it is concluded that both regulations aim to protect the person to whom personal data is related, and that transparency and compliance with the law are important [4].

4. Relationship Between ISO 27001, KVKK and GDPR

ISO 27001, GDPR, and KVKK are information security and data protection standards and regulations that serve different purposes but complement each other or have similar objectives. These standards and regulations have their own purposes, scopes, and application areas. Some of them overlap, while others naturally exhibit differences.

Table 1. Standards and Regulations Comparison: ISO 27001, GDPR, and KVKK

	Purpose	Scope	Application Areas	Sanctions
ISO 27001	It provides a framework for establishing, implementing, monitoring, reviewing, and continuously improving an Information Security Management System (ISMS). Its primary aim is to protect organizations' information assets and make them resilient against cyber threats.	It covers information security management and encompasses all information assets and related processes.	It can be implemented by a wide range of organizations and industries. Any organization can implement ISO 27001 to manage information security risks and protect information assets.	ISO certification demonstrates compliance and often provides a competitive advantage in the market.
KVKK	It includes regulations concerning the processing, protection, and lawful use of personal data in Turkey. Its primary aim is to protect the privacy and security of personal data and ensure their lawful processing.	It covers the processing and protection of personal data in Turkey, affecting all organizations and individuals in Turkey.	All organizations and individuals in Turkey are obligated to comply with KVKK when processing personal data.	Non-compliant organizations with KVKK may also face significant fines. Breaches can be investigated and penalized by the Personal Data Protection Authority (KVKK).
GDPR	It encompasses comprehensive regulation concerning the processing and protection of personal data within the European Union (EU). Its primary aim is to safeguard the privacy and security of individuals' personal data and ensure the lawful processing of such data.	It encompasses the processing and protection of personal data, particularly affecting all organizations processing data of EU citizens.	All organizations, both within and outside the EU, are obligated to comply with GDPR when processing personal data of EU citizens (such as identity information, health data, address, etc.).	Non-compliant organizations with GDPR may face significant fines. Breaches can be investigated and penalized by data protection authorities. Considering the heavy administrative fines adopted by Article 83 of the GDPR, the importance of ensuring GDPR compliance, especially for companies, becomes more evident [6].

4.1 Differences

ISO 27001 regulates information security management, while GDPR and KVKK regulate the protection of personal data. GDPR affects all organizations processing data of EU citizens, while KVKK only affects organizations in Turkey. ISO 27001 is a certification standard, whereas GDPR and KVKK are legal regulations. Additionally, ISO 27001 serves as a certification standard for organizations. Companies can obtain ISO 27001 certification to demonstrate that they have implemented appropriate processes and controls and to showcase this compliance to the external world. Furthermore, GDPR differs from KVKK in several aspects. One such distinction is that under GDPR, Data Processors face much heavier legal liabilities in the event of data breaches compared to KVKK. Additionally, under GDPR, Data Controllers are obliged to oversee the compliance of Data Processors with GDPR [7].

Data controllers are required to monitor and manage data processors' compliance with the terms specified in contracts or other regulations they have signed with them. This regulation aims to ensure that both data controllers and data processors collaborate to secure the security and privacy of personal data and adhere to GDPR provisions effectively.

5. Implementation and Alignment of ISO 27001, GDPR, and KVKK

Integrating ISO 27001, GDPR, and KVKK ensures effective management of both information security and personal data protection practices within an organization. When examining the Data Security Guide published by the Personal Data Protection Board, it is evident that "data security" is directly related to ISMS, which is one of the main headings of KVKK [8]. In the Administrative Measures table in KVKK and in GDPR, the topic of Risk Assessment is present. Given that Risk Assessment is also a fundamental topic in the ISO 27001 standard, it is possible to directly associate the standard with both KVKK and GDPR. Similarly, the requirement of developing policies and procedures in ISO 27001 aligns with the transparency and accountability principles of GDPR. The alignment between the two assists organizations in identifying the necessary steps to comply with GDPR and implementing them [9]. Various approaches exist to ensure this integration in organizations. Various difficulties may be encountered in ensuring integration.In this section, relevant approaches are detailed, potential difficulties are outlined, and evaluated.

Difficulties and Tips for the Harmonization Process:

The process of achieving regulatory compliance can often be time-consuming and complex for businesses. This process consists of several steps and may vary depending on the organization's current status, size, and complexity. Generally, there can be some challenges that organizations may encounter.

Resource Insufficiency: The process of achieving regulatory compliance often requires additional resources. These resources may include time, money, manpower, and expertise. Limited resources, particularly for small and medium-sized enterprises, can make the compliance process challenging.

Complexity: Regulations are often complex and detailed. Understanding and implementing these standards can take time for businesses. Especially if compliance with multiple regulations or standards is required, the complexity can further increase.

Changing Requirements: Regulations can be updated or revised over time. This means that businesses need to continually review and update their compliance processes to meet these changing requirements. Coping with these changing requirements also poses challenges.

Cultural Change: Achieving compliance with regulations often requires changes in organizational culture. Adopting new policies and procedures and educating staff can be a challenge for some businesses, as they may encounter resistance.

Monitoring and Evaluation: The compliance process requires continuous monitoring and evaluation. It is important for businesses to constantly monitor their performance and identify improvement opportunities. However, this can be resource-intensive and time-consuming for some businesses.

External Audits and Certification: In some cases, businesses may need to undergo external audits and obtain certification to verify their compliance with regulations. This process can incur additional costs and time for businesses.

Despite these challenges, the process of regulatory compliance provides long-term benefits for businesses. Compliance with regulations can increase customer trust, provide a competitive advantage, and strengthen the organization in terms of data security. Therefore, it is important for businesses to invest in the compliance process to overcome these challenges.

There are some tips that organizations can apply to cope with these challenges. These tips can make the process of regulatory compliance more manageable and enhance the success of organizations in terms of information security and data protection.

- Starting off on the right foot
- Defining authorities and responsibilities
- Providing training and raising awareness
- Creating a compliance plan
- Embracing a culture of continuous improvement
- Utilizing external resources
- Adopting risk-based approaches
- Strengthening communication

5.1 Determining Common Principles

Taking into account the fundamental principles and requirements of ISO 27001, GDPR, and KVKK, a compliance strategy based on common principles should be established. Some of these common principles include:

- Data Protection and Privacy Principle
- Integrity Principle
- Access Control Principle
- Protection of Rights of Data Subjects
- Risk Management Principle

These common principles represent the core principles and requirements embraced by ISO 27001, GDPR, and KVKK. By adopting and implementing these principles with an integrated approach, organizations can ensure both information security and personal data protection compliance more effectively. Adopting just one principle may be insufficient; relevant standards and regulations should be approached with an integrated strategy and implemented together. This way, more effective compliance with information security and personal data protection can be ensured.

5.2 Risk Management and Checklists

The organization should adopt an integrated risk management approach considering its risk profile and compliance requirements. Risk Management is one of the requirements of these three regulations. Common risks and control lists should be established, and an integrated framework for the controls to be compliant should be developed. In terms of identifying common risks, both ISO 27001 and GDPR compliance requirements entail identifying information security vulnerabilities and taking measures against them, while KVKK and GDPR demand implementing control measures to prevent unauthorized access to personal data. An example table detailing the consolidation of control lists is elaborated in Table 1. below.

Table 2. Consolidation of Control Lists

Control Point	Description	ISO 27001 Compliance	GDPR Compliance	KVKK Compliance

Information Security Policy	Establishment and communication of the organization's information security policy.	X		
Data Access Controls	Implementation of necessary controls to prevent unauthorized access.	X	X	X
Data Breach Notification	Creation of procedures for detecting and reporting potential data breaches.	X	X	X
Employee Training and Awareness	Provision of regular training on information security and personal data protection topics.	X	X	X
Monitoring and Auditing	Regular monitoring and auditing of systems and data processing activities.	X	X	X
Determination of Data Location	Determination and recording of the locations of processed personal data.		X	X
Data Retention Limitations	Implementation of limitations on the retention of personal data for a specified period.	X	X	X

In this example, a control list is provided that includes common control points that can be used to consolidate ISO 27001, GDPR, and KVKK compliance requirements. This list combines the necessary controls for compliance under a single framework, considering the requirements of each compliance area.

5.3 Integrated Policies and Procedures

Creating integrated policies and procedures is of critical importance for ensuring compliance with ISO 27001, GDPR, and KVKK. ISO 27001 requires organizations to develop and implement information security policies and procedures [9].

These policies and procedures provide a framework that combines both information security management and personal data protection practices, encouraging a cohesive approach to compliance. Information security policies and personal data protection policies should be developed with an approach that integrates compliance requirements. Common procedures should be established, ensuring consistency across practices. These policies and procedures:

- They should encompass both information security and personal data protection principles.
- The information security policy should cover fundamental information security topics such as protection of information assets, access control, encryption, and security measures like firewalls.
- Personal data protection procedures should be created in accordance with KVKK and GDPR requirements, addressing aspects like collection, storage, use, sharing, and disposal of personal data.

5.4 Training and Awareness Programs

Training and awareness programs for employees should be integrated to cover both information security and personal data protection topics. Common training materials and awareness campaigns should be developed. Organizations should assess the training needs of employees, considering ISO 27001, GDPR, and KVKK requirements. These programs should include topics such as basic information security principles, protection of information assets, data privacy, authorization, and authentication. Additionally, personal data protection training should encompass KVKK and GDPR requirements and principles of personal data processing. Using exams and assessment tools, employees' knowledge levels can be measured, and the effectiveness of the training can be evaluated. Example training program is detailed in Table 2. Ensuring involvement and commitments from senior management in training and awareness programs can encourage employee participation and the establishment of a culture of information security.

Table 3. Example Training Program

Training Title	Description	Target Audience	Duration
Basic Information Security Principles	An introduction to basic concepts and importance of information security.	All employees	1 hour
Protection of Information Assets	Protection and management of information assets within the organization.	All employees	2 hour
Data Privacy	Importance of data privacy and protection of personal and sensitive data.	All employees	1.5 hour
Authorization and Authentication	Access control mechanisms and methods for verifying user identities.	IT personnel, system administrators	2 hour
KVKK Fundamental Principles	Basic principles of KVKK and personal data protection topics.	All employees	1.5 hour
GDPR Practices	GDPR requirements and principles of personal data processing.	All employees	2 hour
Crisis Management and Incident Response	Effective response strategies in the event of information security breaches or crisis situations.	Executive Level Management	2.5 hour
Risk Management and Strategic Planning	Determination of organizational risk management strategies and integration of information security strategy.	Executive Level Management	2.5 hour
Legal and Regulatory Requirements	General overview of key legal regulations such as ISO 27001, GDPR, and KVKK requirements and their implementation.	Executive Level Management	2 hour

In this example, a training program is proposed targeting both senior executives and all employees. These trainings aim to assist executives in determining and implementing the organization's information security and personal data protection strategies, while also catering to the needs of all employees and aiming for participants to have varying levels of knowledge.

5.5 Monitoring and Improvement Processes

These processes enable the organization to effectively manage its compliance process, monitor its performance, and continuously improve. Integrated monitoring and internal audit processes should be established to assess the effectiveness of the compliance process. Improvement activities should be managed using common criteria and performance indicators applicable to both areas. The examples related to the processes are detailed in Table 3.

Table 4. Monitoring, Improvement, and Performance Indicator Processes

Process	Description	Performance Indicators	Common Metrics	Responsible Departments
Audit and Monitoring Plan Creation	Establishment of an annual audit and monitoring plan to ensure compliance with ISO 27001, GDPR, and KVKK. The plan involves regular monitoring, auditing, and evaluation of identified compliance requirements.	Level of implementation of the audit plan, number of completed audits, status of identified action items.	Compliance rate, implementation rate of action items	Information Security Department, Internal Audit Department
Incident and Breach Monitoring	Process established for monitoring and reporting incidents and breaches. It ensures the rapid detection of any security breach or data leakage and the implementation of appropriate measures.	Time to detect and respond to incidents, time to resolve incidents, number of breach reports.	Incident detection rate, response time	Information Security Department, Business Continuity and Risk Management Unit
Continuous Improvement Meetings	Regular meetings held to discuss identified areas for improvement. Improvement opportunities are identified based on monitoring results, improvement plans are developed, and implemented.	Rate of implementation of identified improvement activities, number of completed improvement projects, participation rate in meetings.	Effectiveness of improvement activities, success of improvement projects	Quality and Compliance Department, Internal Audit Department
Evaluation of Training Programs	Regular assessment of employee training and awareness levels. The effectiveness and participation levels of training programs are reviewed, and improvements are made as necessary.	Number of completed trainings, participation rate, employee feedback.	Training effectiveness, participation rates	Human Resources Department, Quality and Compliance Department
Performance Metrics Tracking	Regular monitoring of defined performance metrics and evaluation of performance. These metrics are used to determine the effectiveness of compliance processes, the status of achieving objectives, and the necessity of continuous improvement.	Performance metrics tracking, performance evaluation.	Compliance effectiveness, achievement status, need for continuous improvement.	Quality and Compliance Department, Business Continuity and Risk Management Unit

5.6 External Audits and Certifications

External audits and certifications are critical processes for ensuring compliance with ISO 27001, GDPR, and KVKK. These processes are used to assess the organization's level of compliance, verify its compliance through an external independent review, and demonstrate its compliance to customers or regulatory authorities. When necessary, both ISO 27001 and GDPR and KVKK compliance should be subjected to external independent audits and certification. These audits are important for verifying the effectiveness of the compliance process and promoting continuous improvement. The certification process not only demonstrates the organization's compliance to customers, suppliers, partners, and other stakeholders but also enhances the organization's credibility and can provide a competitive advantage in business relationships.

These approaches represent different strategic steps that can be used to integrate ISO 27001, GDPR, and KVKK compliance. Organizations can adapt these approaches according to their needs and requirements, enabling them to manage the compliance process more effectively.

6. Conclusion

ISO 27001, GDPR, and KVKK underline the interconnection between information security management and personal data protection, emphasizing their relationship. While ISO 27001 aims to establish a robust information security management system, GDPR and KVKK encompass the protection of personal data and the rights of individuals. Despite the differences among these standards and regulations, they share common principles and objectives, enabling organizations to integrate their compliance efforts effectively.

Achieving compliance with ISO 27001, GDPR, and KVKK requires a strategic approach that harmonizes policies, procedures, and training programs. Identifying common principles, adopting integrated risk management practices, and establishing consistent policies and procedures allow organizations to effectively manage their compliance obligations. Thus, organizations not only strengthen their position in terms of information security but also ensure compliance with legal regulations.

However, organizations may encounter difficulties in the process of achieving regulatory compliance, such as resource constraints, complexity, changing requirements, and cultural shifts. To overcome these challenges, organizations should prioritize education, develop a compliance plan, embrace a culture of continuous improvement, and utilize external resources when necessary.

In conclusion, understanding and implementing the ISO 27001:2022 standard provides a strong foundation for both information security and personal data protection. These standards help businesses establish a secure and compliant data management culture, making them more resilient against cybersecurity threats. By proactively addressing information security and data protection concerns, organizations can effectively navigate the evolving landscape of regulatory requirements and protect sensitive information. As a result of these approaches, businesses can increase customer trust, gain a competitive advantage, enhance data security, reduce operational risks, and ensure long-term sustainability. These steps shed light on businesses successfully managing the process of regulatory compliance and gaining a competitive edge.

References

[1] Çetinkaya, M. (2008). Kurumlarda Bilgi Güvenliği Yönetim Sistemi'nin Uygulanması. Akademik Bilişim 2008 , 511-516.

[2] Yılmaz, H. (2014). Ts Iso/Iec 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması Ve Bilgi Güvenliği Risk Analizi. Denetişim, 45-59.

[3] Meral S., Bülbül H.İ. (2022). Analysis Of The Efficiency Of The Information Security Policies Of Public Institutions İn Terms Of Ensuring Corporate Information Security. Fen Bilimleri Dergisi, 314-329.

[4] Savaş, R.N., Zaim, A. H., Aydın, M. A. (2020). Kvkk Ve Gdpr Kapsamında Firmaların Mevcut Durum Analizi Üzerine Bir İnceleme. İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi, 208-223.

[5] Kvkp (2020, Accessed On 12.05.2024). Retrieved From Https://Www.Kisiselverilerinkorunmasi.Org/Mevzuat/Avrupa-Birligi-Genel-Veri-Koruma-Tuzugu-Gdpr-Turkce-Ceviri/

[6] Dülger, M. V. (2019). Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması. Yaşar Hukuk Dergisi C.1 S.2 , 71-174.

[7] Olca, E. A., Can, Ö. (2024). Kvkk Kavramlarının Modellenmesi İçin Ontoloji Tabanlı Bir Yaklaşım. Dokuz Eylül Üniversitesi Mühendislik Fakültesi Fen Ve Mühendislik Dergisi, 173-191.

[8] Tosunoğlu, A. (Accessed On 13.05.2024). Iso/Iec 27001 Bilgi Güvenliği Yönetim Sistemi'nin Kvkk'ya Etkisi. Retrieved From Proks Certification: Https://Proks.Co/Haberler/İso-İec-27001-Bilgi-Guvenligi-Yonetim-Sistemi-Nin-Kvkk-Ya-Etkisi

[9] Kılıç, B. (2024). Kuruluşların Başarısı İçin Iso 27001 Ve Kişisel Verilerin Korunması. 3. Nesil Hukuk Dergisi.

[10] Evren, A. G. (2023). Avrupa Birliği Ve Türkiye Kişisel Verilerin Korunması Kanunlarının Karşılaştırmalı Analizi: Temel İlkeler, Yasal Dayanaklar Ve İlgili Kişi Hakları. Kişisel Verileri Koruma Dergisi, 39-64.