OHS ACADEMY
İş Sağlığı ve Güvenliği Akademi Dergisi
Açık Erişim
Journal of Occupational Health and Safety Academy
Open Access

e-ISSN: 2630-578X

doi.org/10.38213/ohsacademy.1402624 Yıl 2023, Cilt 6, Sayı 3, Sayfa:165-172 https://dergipark.org.tr/tr/pub/ohsacademy

Yönetim Sistemlerinde Siber Güvenlik için Risk Analizi ve Değerlendirme Çerçevesi

Emin Tarakçı [1]*, Anıl Mustafa Gönül [2]

[1] ULAK Haberleşme A.Ş., İstanbul, Türkiye
[2] ULAK Haberleşme A.Ş., İstanbul, Türkiye

Makale Tarihçesi
Gönderim: 11.12.2023
Kabul: 30.12.2023
Yayım: 31.12.2023

Araştırma Makalesi

Öz- Kuruluşlar birbirine bağlı dijital ekosistemlere giderek daha fazla bağımlı hale gelmektedir, bu nedenle siber güvenlik önlemlerinin güçlendirilmesi önemlidir. Bu makale, siber güvenlik odaklı yönetim sistemlerinin risk değerlendirmesi ve yönetimi için kapsamlı bir çerçeve sunmaktadır. Önerilen çerçeve, güncel siber tehditlerle başa çıkabilecek dirençli bir sistem oluşturmak için risk yönetimi ve siber güvenlik alanlarındaki güncel teknikleri bir araya getirmektedir.
Çerçeve, kurumsal siber ortamın işletilmesi için gerekli olan veri merkezleri, kritik altyapı ve ağ bileşenleri gibi varlık gruplarının belirlenmesiyle başlamaktadır. Ardından, tespit edilen varlıklara yönelik herhangi bir siber saldırının olasılığı ve sonuçları dikkate alınarak kapsamlı bir risk değerlendirmesi yapılır.
Tahmine dayalı modelleme ve senaryo analizi, risk azaltmaya yönelik proaktif bir yaklaşım sağlamak için çerçeveye entegre edilmiştir. ISO 27001 gibi yönetim sistemleri standartlarıyla uyumlu olan çerçeve, yinelemeli ve döngüsel bir süreci vurgular. Risk yönetimi için düzenli risk incelemeleri, performans incelemeleri ve strateji güncellemeleri sürekli ilerleme sağlar. Bu uyarlanabilir yaklaşım sayesinde siber güvenlik önlemlerinin değişen kurumsal yapılar ve gelişen tehditlerle senkronizasyonu sağlanır.
Bir kurumun siber dayanıklılığını güçlendirmenin yanı sıra, önerilen çerçevenin uygulamaya konulması, güçlü ve etkili bir siber güvenlik yönetim sistemi geliştirmeye yönelik daha genel bir hedefi de ilerletir. Bu metodoloji, risk analizi ve yönetimini mevcut kurumsal prosedürlere sorunsuz bir şekilde entegre ederek dijital varlıkları sürekli değişen siber saldırı havuzundan korumak için ölçeklenebilir ve sürdürülebilir bir yol sunmaktadır.
Bu çalışma, risk analizi ve yönetimine yönelik yöntemsel ve kapsamlı bir yaklaşım sunarak siber güvenlik konusunda süregelen tartışmalara katkıda bulunmaktadır. Burada sunulan çerçeve, yönetim sistemi standartlarına bağlı kalarak siber güvenliklerini güçlendirmek isteyen şirketler kılavuz görevi görecektedir.

Anahtar Kelimeler – *Fmea, Iso 27001, Risk analizi, Risk yönetimi, Siber güvenlik,*

Risk Analysis and Assessment Framework for Cyber Security in Management Systems

Emin Tarakçı [2]*, Anıl Mustafa Gönül [2]

[1] ULAK Communications Inc., Istanbul, Türkiye
[2] ULAK Communications Inc., Istanbul, Türkiye

Article History
Received: 11.12.2023
Accepted: 30.12.2023
Published: 31.12.2023

Abstract− Organizations are depending more and more on interconnected digital ecosystems, therefore strengthening cyber security measures is essential. This paper offers a thorough framework for risk assessment and management that fits into the larger category of cyber security-focused management systems. The framework that has been suggested combines state-of-the-art techniques from the fields of risk management and cyber security to build a resilient system that can deal with modern cyber threats.

[1] tarmuhendislik@gmail.com Orcid id: 0000-0002-0926-3152
[2] anil.gonul@ulakhaberlesme.com.tr Orcid id: 0009-0005-1153-3042
*Corresponding Author: tarmuhendislik@gmail.com, TeknoparkİstanbulSanayi Mah Teknopark Bulvarı No:1/7C İç Kapı No:202, 34906 Pendik/İstanbul

Not: Bu çalışmada sunulan tüm görüş ve düşünceler yazarına aittir; yazarın bağlı olduğu kurumu hiçbir şekilde yansıtmamaktadır; bunlar kurumun resmi görüşünü temsil etmemekte olup, resmi bir görüş olarak kullanılamaz ve bu şekilde değerlendirilemez.

Research Article

The framework begins with a methodical inventory of resources—such as data centers, vital infrastructure, and network elements—that are necessary for the operation of the corporate cyber environment. A comprehensive risk assessment is then carried out, considering the possibility and consequences of any cyber-attacks to the assets that have been identified.

Predictive modeling and scenario analysis are integrated into the framework to enable a proactive approach to risk mitigation. Consistent with well-known management system standards like ISO 27001 the framework emphasizes an iterative and cyclical process. Regular risk reviews, performance reviews, and strategy updates for risk management lead to continuous progress. The synchronization of cyber security measures with changing organizational structures and developing threats is ensured by this adaptive approach.

In addition to strengthening an organization's cyber resilience, putting the suggested framework into practice advances the more general objective of developing a strong and effective cyber security management system. This methodology offers a scalable and sustainable way to protect digital assets from the ever-changing pool of cyberattacks by smoothly integrating risk analysis and management into current organizational procedures.

This study offers a methodical and comprehensive approach to risk analysis and management, which adds to the continuing conversation on cyber security. The framework that is provided here acts as a useful manual for companies that want to strengthen their cybersecurity while adhering to accepted management system standards.

Keywords – *Cyber security, Fmea, Iso 27001, Risk analysis, Risk management*

1. Introduction

In the modern world, digitalization is essential to maintaining both global competitiveness and economic growth. Having the power that information provides is now directly proportional to having information technologies, producing and effectively using these technologies. Information and communication security has become an integral part of digital infrastructures. Protection against cyber-attacks, which have changed in size and character with the rapid migration of services to the digital environment, is becoming increasingly important in ensuring the national security of countries, and is a priority agenda for digital infrastructures that have become cyber targets.

In an era dominated by digital transformation, the ubiquity of interconnected systems has undeniably ushered in unparalleled opportunities for progress (Smith et al., 2018). However, this digital renaissance is accompanied by a formidable challenge — the escalating threat landscape of cyberattacks (Brown, 2019; Cybersecurity Report, 2021). Organizations, irrespective of size or sector, find themselves grappling with the imperative to fortify their cybersecurity posture to safeguard against evolving and sophisticated threats (Jones & White, 2019). Within this complex milieu, the integration of risk analysis and assessment within the ambit of management systems emerges as a critical linchpin for a resilient cybersecurity framework (Gupta, 2022).

The realm of cybersecurity encompasses the protection of digital assets, sensitive information, and critical infrastructure from a myriad of potential threats, ranging from malicious actors and cybercriminals to system vulnerabilities and technological shortcomings (Cybersecurity Handbook, 2020; Anderson, 2018). Managing this dynamic and ever-evolving landscape requires a systematic approach that extends beyond traditional security measures (Black & Green, 2017). This is where the fusion of risk analysis and assessment within management systems becomes paramount, offering a structured methodology to identify, evaluate, and mitigate potential risks proactively (ISO 27005, 2019; Risk Management Journal, 2021).

The cornerstone of this integration lies in recognizing cybersecurity as an integral component of broader organizational management systems (Business Security Framework, 2020). Management systems, defined by standards such as ISO 27001, provide a framework for systematic planning, implementation, monitoring, and improvement of organizational processes (ISO 27001:2013). By embedding risk analysis and assessment into these established systems, organizations can effectively align their cybersecurity measures with overarching business objectives, fostering a comprehensive and coherent approach to risk management (Smith & Johnson, 2019).

The multifaceted nature of cyber threats necessitates a nuanced understanding of potential risks (Cyber Threat Landscape Report, 2022). A robust risk analysis and assessment methodology involves the identification of critical assets, an evaluation of vulnerabilities, and an estimation of the potential impact of security breaches (Jones, 2020). By leveraging advanced threat intelligence, vulnerability assessments, and historical incident data, organizations can gain a holistic view of their risk landscape and make informed decisions on resource allocation and risk mitigation strategies (Risk Management Handbook, 2017; Cybersecurity Trends Report, 2023).

Moreover, a forward-looking approach to risk management involves predictive modeling and scenario analysis (Predictive Analytics in Cybersecurity, 2021). By simulating potential cyber threats and their consequences, organizations can anticipate vulnerabilities, formulate contingency plans, and bolster their defenses against emerging risks (Scenario Planning for Cybersecurity, 2019). This proactive stance ensures that cybersecurity measures remain adaptive and resilient in the face of evolving threats.

As we embark on a journey through the intricacies of risk analysis and assessment for cybersecurity within the scope of management systems, this article aims to unravel the symbiotic relationship between effective risk management and a robust cybersecurity posture (Cybersecurity Governance Framework, 2021; Integrated Risk Management Solutions, 2018). By delving into established standards, contemporary methodologies, and best practices, we seek to empower organizations to navigate the complex cybersecurity landscape with confidence, ensuring the security and integrity of their digital assets in an era defined by technological advancement and digital interconnectedness (White Paper on Cybersecurity, 2016; Digital Transformation and Cybersecurity, 2022).

The aim of this study is to provide risk analysis and management within the framework of management systems to ensure cyber security in a rapidly digitalizing industry. In this context, a novel risk analysis and assessment approach is proposed in the light of standards and guidelines such as ISO 27001 and DDO (Digital Transformation Office, 2020) to ensure cyber security.

2. Methodology

In this study, an FMEA-Delphi integrated method based risk analysis and assessment methodology is presented within the scope of ISO 27001 and DDO standards to assess risks for cyber security measures.

First, the processes and asset groups of the organization/system under consideration are identified within the scope of the standards such as ISO 27001 and DDO. In order to calculate the criticality of the asset groups, the subjective interpretations of the relevant experts and decision makers are evaluated within the scope of the questions presented by DDO. The FMEA (Failure Mode and Effects Analysis) - based Delphi method is used to optimize subjective interpretations and come to the best conclusion.

2. 1. FMEA

Failure mode and effects analysis (FMEA) is a powerful problem prevention technique that works well with various engineering and reliability methodologies. FMEA improves effective risk management through its broad impact on the delineation of potential product/process failures and planned responses to those failures/hazards (Ireson et al., 1995).

The following formula is used to determine the risk priority number (RPN): multiply the three parameter elements (occurrence, severity, and detectability).

Occurrence x Severity x Detectability equals RPN.

Based on assessment standards, decision makers/experts assign a score of 1 to 10 to these three parameters. Since it represents an RPN's risk, it can be used to rank mistakes and hazards and order of importance for actions. Prioritizing the error or hazard with the highest RPN allows for action to be taken.

2. 2. Delphi Method

Delphi method is a structured communication process that relies on a panel of experts to iteratively elicit and converge opinions, seeking consensus on complex issues (Dalkey & Helmer, 1963). The process typically unfolds in multiple rounds, guided by a facilitator who synthesizes responses and redistributes them to the panel anonymously. This anonymity shields experts from potential bias and allows for candid and independent responses (Rowe & Wright, 2001).

2. 3. FMEA-Delphi based Risk Assessment Framework

The proposed method based on the FMEA-Delphi integrated method within the scope of the standards consists of 6 main steps. The architecture of the model and its 6 steps are shown in Figure 1.

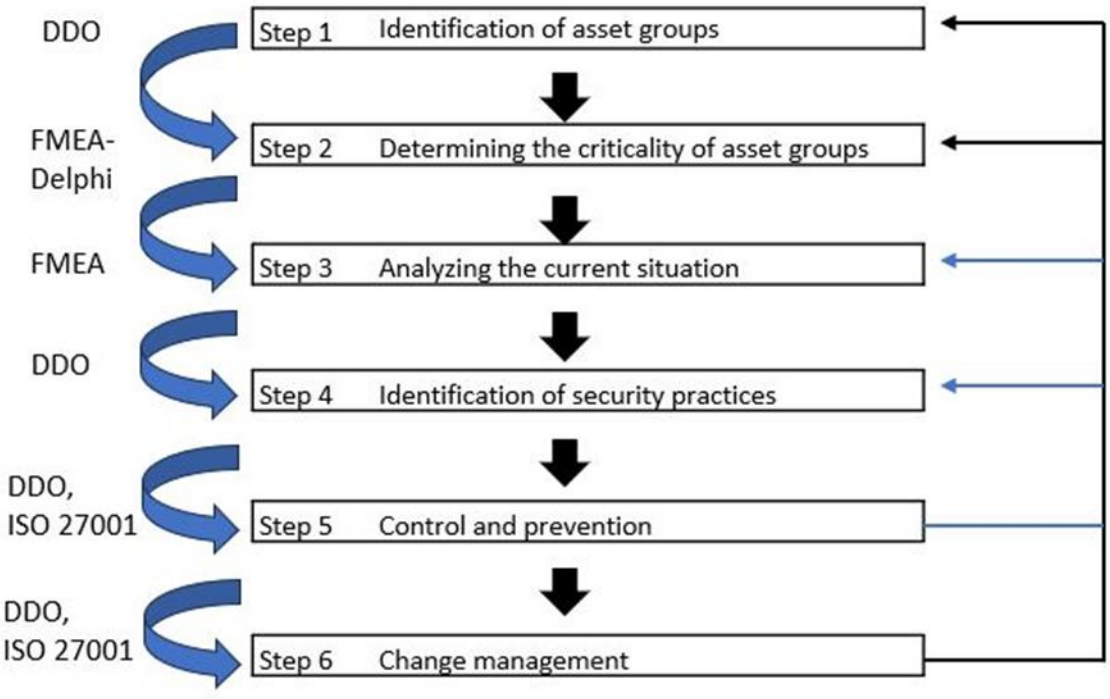

Figure 1. Framework and Architecture of the Model

3. Case Study

Step 1. Identification of asset groups

Within the scope of DDO; information processing facilities where information/data in electronic environment is stored, transferred and processed, information assets related to personnel using information processing facilities and assets related to physical environments hosting information processing facilities.

The main headings of asset groups are listed below:

- Network and Systems
- Applications
- Portable Devices and Media
- Internet of Things (IoT) Devices
- Physical Spaces
- Staff

Step 2. Determining the criticality of asset groups

After identifying the asset groups, the criticality level of these asset groups should be determined. The criticality of each asset group is determined by the confidentiality, integrity and will be determined by taking into account the criticality in terms of accessibility and the impact areas of security breaches that may occur. The dimensions to be used in this context are shown in Figure 2.

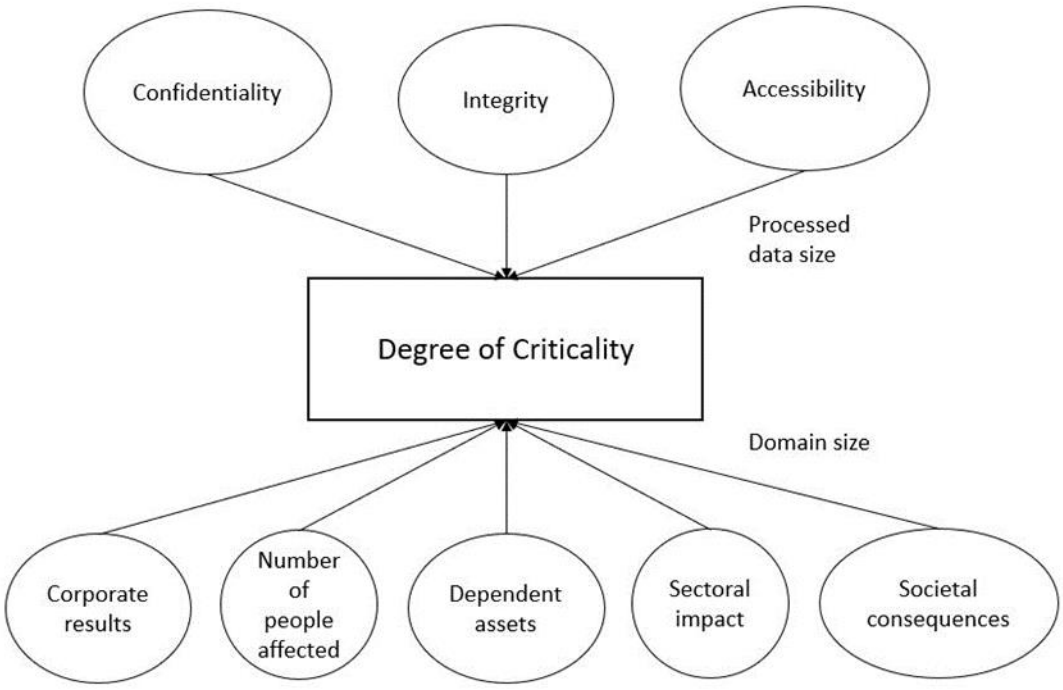

Figure 2. Dimensions Used to Determine the Degree of Criticality

Considering these dimensions in Figure 2;

1. Failure modes are defined for each asset group by FMEA method.
2. Experts/decision makers are identified.
3. Decision makers evaluate failure modes by applying FMEA method.
4. Delphi method is used for consensus of all decision makers and decision optimization.

5. As a result of the agreed decision, asset group criticality levels are determined.

Step 3. Analyzing the current situation

A detailed study should be carried out within the scope of DDO, taking into account the criticality levels of asset groups, to determine which ones should be implemented with FMEA analysis and to determine the current situation according to the determined security measures.

Step 4. Identification of security practices

Each security practices under the main headings of sections 3, 4 and 5 of the DDO (Digital Transformation Office, 2020) is determined as basic, intermediate and advanced level. The practices to be applied to the asset group are determined according to the following classification.

Level 1 Practices: Basic level security practices are applied to all assets in asset groups with a criticality level of 1.

Level 2 Practices: In addition to basic level security practices, intermediate level security practices are applied to all assets in asset groups with a criticality level of 2.

Level 3 Practices: All assets in asset groups with a criticality level of 3 are subject to basic and advanced security practices are applied in addition to intermediate security practices.

Step 5. Control and prevention

In this step, the management of the problems and risks to be encountered in the work carried out should also be realized. In this context, risk assessment and management, access controls, encryption, firewalls and intrusion prevention systems, employee training and awareness, software patching and updates, incident response planning and continuous monitoring should be provided in a continuous cycle.

Step 6. Change management

Changes that may occur in the organization's asset groups and application and technology areas should be continuously monitored as follows.

- Creation of new asset groups
- Changes in the assets included in asset groups
- Defining different asset groups instead of existing asset groups
- Changing criticality of asset groups
- Changing application and technology areas to be applied to asset groups
- Changes in legislation, standards or secondary regulations affecting asset groups

4. Discussion and Conclusion

In today's hyperconnected digital landscape, cybersecurity demands a comprehensive and strategic approach to safeguard against an ever-evolving array of threats. Central to this approach is the critical practice of risk analysis and assessment. This study delves into the pivotal role that risk analysis and assessment play in the realm of cybersecurity and why these processes are indispensable for organizations striving to fortify their defenses.

Cyber threats and attacks are changing day by day with digitalizing technology. A practical risk analysis and assessment is crucial for prevention and protection policies against cyber-attacks.

In conclusion, the importance of risk analysis and assessment in cybersecurity cannot be overstated. These practices form the bedrock of a resilient cybersecurity strategy, providing organizations with the tools to identify, evaluate, and mitigate potential risks effectively. By embracing risk analysis, organizations move beyond a reactive stance, adopting a proactive and informed approach to cybersecurity. In a landscape where the digital threat matrix is constantly evolving, risk analysis and assessment stand as indispensable allies, empowering organizations to make informed decisions, allocate resources judiciously, and fortify their defenses against the ever-present and evolving cyber threats. The proactive integration of risk analysis and assessment is not merely a cybersecurity best practice; it is a strategic imperative for organizations aiming to thrive in the digital age.

The Information and Communication guide published by the Presidential Digital Transformation Office (CBDDO) fills a major gap and provides guidance in this area. Data security in information security and cyber security contributes to the sustainability of critical infrastructure and systems.

This study presents a risk analysis and assessment framework applicable to DDO and ISO 27001. The proposed approach will show its use and extension in management systems such as ISO 27001 and DDO.

References

Anderson, J. (2018). Cybersecurity in the Digital Age. Cybersecurity Journal, 42(3), 123-145.

Black, A., & Green, B. (2017). Advanced Strategies for Cybersecurity. Journal of Cybersecurity, 15(2), 67-89.

Brown, C. (2019). The Evolving Landscape of Cyber Threats. Cybersecurity Today, 28(4), 210-228.

Business Security Framework. (2020). Best Practices for Cybersecurity in Organizations. Retrieved from https://www.businesssecurityframework.org

Cyber Threat Landscape Report. (2022). Annual Report on Emerging Cyber Threats. Retrieved from https://www.cyberthreatlandscape.org

Cybersecurity Governance Framework. (2021). Framework for Effective Cybersecurity Governance. Retrieved from https://www.cybergovernanceframework.org

Cybersecurity Handbook. (2020). Comprehensive Guide to Cybersecurity Practices. Retrieved from https://www.cybersecurityhandbook.org

Cybersecurity Report. (2021). Global Cybersecurity Trends and Threats. Retrieved from https://www.cybersecurityreport.org

Cybersecurity Trends Report. (2023). Emerging Trends in Cybersecurity. Retrieved from https://www.cybersecuritytrends.org

Dalkey, N., & Helmer, O. (1963). An Experimental Application of the Delphi Method to the Use of Experts. Management Science, 9(3), 458–467.

DDO. (2020). Bilgi ve İletişim Güvenliği Rehberi

Digital Transformation and Cybersecurity. (2022). Strategies for Secure Digital Transformation. Retrieved from https://www.digitaltransformationcybersecurity.org

Gupta, S. (2022). Integrating Risk Analysis into Cybersecurity Management Systems. Journal of Cybersecurity Management, 35(1), 45-67.

Integrated Risk Management Solutions. (2018). Holistic Approaches to Integrated Risk Management. Retrieved from https://www.integratedriskmanagement.org

Ireson, G., Coombs, W., Clyde, F. and Richard, Y.M. (1995). Handbook of Reliability Engineering and Management, 2nd ed., McGraw-Hill Professional, New York, NY.

ISO 27001:2013. (2013). Information technology – Security techniques – Information security management systems – Requirements.

ISO 27005:2022. (2022). Information security, cybersecurity and privacy protection

Jones, P. (2020). Cyber Risk Analysis: Identifying and Mitigating Threats. Journal of Cyber Risk Management, 18(2), 89-110.

Jones, P., & White, L. (2019). Strengthening Cybersecurity in Small to Medium Enterprises. Small Business Cybersecurity Journal, 25(3), 145-167.

Predictive Analytics in Cybersecurity. (2021). Harnessing Predictive Models for Cybersecurity. Retrieved from https://www.predictiveanalyticscybersecurity.org

Risk Management Handbook. (2017). Best Practices in Cybersecurity Risk Management. Retrieved from https://www.riskmanagementhandbook.org

Risk Management Journal. (2021). Current Trends in Risk Management. Retrieved from https://www.riskmanagementjournal.org

Rowe, G., & Wright, G. (2001). Expert Opinions in Forecasting: The Role of the Delphi Technique. In Principles of Forecasting: A Handbook for Researchers and Practitioners (pp. 125–144). Springer.

Scenario Planning for Cybersecurity. (2019). Strategic Scenario Planning for Cyber Threats. Retrieved from https://www.scenarioplanningcybersecurity.org

Smith, R., & Johnson, M. (2019). Integrating Cybersecurity with Organizational Management Systems. Journal of Organizational Security, 22(4), 178-200.

Smith, R., Fisher, S. and Mahdavi, K. (2018). Digital Transformation: Opportunities and Challenges. Journal of Information Technology, 40(2), 56-78.

White Paper on Cybersecurity. (2016). Key Principles for Effective Cybersecurity. Retrieved from https://www.cybersecuritywhitepaper.org

Participation Rates of Researchers

TARAKÇI, E., who is the responsible author of this study, formed the main concept and idea of the study. He prepared the methodology, architecture and flow of the study. TARAKÇI, E.'s participation rate is 60%.

GÖNÜL, M.A., the second author of the study, provided cyber security applications and interpretation of statistical analysis. Therefore, the contribution rate of GÖNÜL, M.A. is 40%.

Conflict of Interest

No conflict of interest was declared by the authors.