DOI: https://doi.org/10.36719/2789-6919/56/160-164

Rovshan Taghiyev
Nakhchivan State University
https://orcid.org/0000-0002-3682-8788
rovsentagiyev@ndu.edu.az
Rana Kalashova
Nakhchivan State University
https://orcid.org/0009-0008-2768-7240
renaa162010@gmail.com

The Relationship Between Information Systems and Information Technologies, and Ensuring Their Security

Abstract

In modern organizations, the integration of Information Systems and Information Technologies plays a critical role in supporting information management, optimizing business processes, and achieving strategic objectives. Information Systems provide the framework for collecting, processing, and analyzing data, while Information Technologies supply the tools and infrastructure that enable these systems to function effectively. The effectiveness of this relationship, however, is highly dependent on the security of information systems. This study examines key aspects of IS and IT security, including the prevention of unauthorized access, protection of data integrity, implementation of security policies and standards, system and network security, disaster recovery and business continuity planning, and protection against cyber threats. IT auditing is highlighted as an essential mechanism for evaluating organizational defenses, identifying vulnerabilities, and recommending improvements.

Keywords: *information systems, information technology, cybersecurity, IT auditing, business continuity*

Rövşən Tağıyev
Naxçıvan Dövlət Universiteti
https://orcid.org/0000-0002-3682-8788
rovsentagiyev@ndu.edu.az
Rəna Kalaşova
Naxçıvan Dövlət Universiteti
https://orcid.org/0009-0008-2768-7240
renaa162010@gmail.com

İnformasiya Sistemləri və İnformasiya Texnologiyaları arasında əlaqələr və onların təhlükəsizliyinin təmin edilməsi

Xülasə

Müasir təşkilatlarda İnformasiya Sistemləri və İnformasiya Texnologiyalarının inteqrasiyası informasiya idarəçiliyinin dəstəklənməsi, biznes proseslərinin optimallaşdırılması və strateji məqsədlərə nail olunmasında mühüm rol oynayır. İnformasiya Sistemləri məlumatların toplanması, işlənməsi və təhlili üçün çərçivə təmin edir, İnformasiya Texnologiyaları isə bu sistemlərin effektiv işləməsini təmin edən alətlər və infrastrukturu təmin edir. Bununla belə, bu əlaqənin effektivliyi informasiya sistemlərinin təhlükəsizliyindən çox asılıdır.

Bu tədqiqat İS və İT təhlükəsizliyinin əsas aspektlərini, o cümlədən icazəsiz girişin qarşısının alınması, məlumatların bütövlüyünün qorunması, təhlükəsizlik siyasətlərinin və standartlarının həyata keçirilməsi, sistem və şəbəkə təhlükəsizliyi, fəlakətlərin bərpası və biznesin davamlılığının planlaşdırılması və kiber təhdidlərdən müdafiəni araşdırır. İT auditi təşkilati müdafiənin qiymətləndirilməsi, zəifliklərin müəyyən edilməsi və təkmilləşdirmələrin tövsiyə edilməsi üçün vacib mexanizm kimi vurğulanır.

Açar sözlər: *informasiya sistemləri, informasiya texnologiyaları, kibertəhlükəsizlik, İT auditi, biznesin davamlılığı*

Introduction

In today's digital era, organizations increasingly rely on information systems (IS) and information technologies (IT) to manage data, optimize business processes, and achieve strategic objectives. The integration of IS and IT has become a critical determinant of organizational efficiency, competitiveness, and innovation. Information systems provide a structured framework for the collection, processing, storage, and analysis of data, while information technologies encompass the hardware, software, networks, and infrastructure necessary to ensure the effective operation of these systems. However, the growing dependence on digital systems also exposes organizations to a wide range of internal and external threats. Cyberattacks, unauthorized access, data corruption, and system failures can disrupt operations, compromise sensitive information, and undermine organizational resilience. Consequently, ensuring the security of information systems is essential not only for operational continuity but also for maintaining stakeholder trust and achieving long-term organizational goals.

This study explores the relationship between IS and IT and emphasizes the importance of securing information systems through comprehensive IT auditing, risk management, and the implementation of security policies and standards. By examining key areas such as access control, data integrity, system and network protection, disaster recovery, and cyber threat mitigation, this research highlights the critical role of security in sustaining efficient, reliable, and resilient organizational operations.

Research

The Relationship Between Information Systems and Information Technologies. Information Systems and Information Technologies are two critical components that support information management and optimize business processes in modern organizations. These two concepts are complementary in nature and, when used effectively, enable the achievement of organizational objectives. While information systems provide a framework for the collection, processing, and analysis of data, information technologies represent the tools and infrastructure that make the operation of these systems possible (Laudon & Laudon, 2020).

Information Systems are a combination of processes, tools, and human elements designed to support information management within organizations. They encompass the processes of data collection, processing, and analysis. In contrast, Information Technology refers to a structure that includes hardware, software, networks, and data storage technologies, providing the necessary infrastructure for the operation of information systems (Zhang et.al., 2023).

The relationship between information systems and information technologies can be explained through the analogy of a *"car"* and an *"engine."* While information systems represent the body and mechanisms of a car, information technologies function as the engine that enables the system to operate. This relationship can be clearly observed in the following areas:

– *Data Processing and Management:* IS transforms raw data into meaningful information, whereas IT provides the tools that accelerate and optimize this process. For example, database management systems (DBMS) clearly demonstrate this relationship (Dragomir, 2017).

– *Decision-Making Processes:* Management Information Systems (MIS) utilize IT infrastructure to support organizational decision-making. Analytical tools and big data platforms enhance effectiveness in this area (Nguyen et al., 2020).

– *Automation of Business Processes:* While business processes are defined and optimized by IS, IT enables the automation of these processes. For instance, Enterprise Resource Planning (ERP) systems use IT to integrate business processes.

The relationship between information systems and information technologies is also strongly evident at the component level, as outlined below:

– *Hardware and Software:* Hardware and software are fundamental components of Information Technology that provide the necessary support for the functioning of Information Systems. Hardware includes physical devices such as servers, computers, storage units, and networking equipment, which facilitate data processing, storage, and transmission. Software encompasses operating systems, application programs, and specialized tools that manage, process, and analyze data. Together, hardware and software form the backbone of IT infrastructure, enabling information systems to operate efficiently, handle large volumes of data, and support organizational decision-making and business operations (Caldwell, 2009).

– *Data and Data Analytics*: Information Systems transform raw data into meaningful and actionable information, which organizations can use for strategic decision-making and performance improvement. Information Technology enhances this process by providing advanced tools for data analytics, including big data platforms, machine learning algorithms, and data mining techniques. These technologies allow organizations to process complex datasets, identify patterns, detect anomalies, and generate predictive insights, thereby increasing the value and accuracy of the information produced (Yoon, 2015).

– *People and Processes:* Information Systems define, structure, and manage organizational processes, ensuring that workflows are standardized, efficient, and aligned with business objectives. Information Technology complements this by enabling the implementation and automation of these processes through software applications, workflow management systems, and digital platforms. By combining human expertise with IT tools, organizations can optimize operations, reduce manual errors, enhance collaboration, and respond more quickly to changing business demands, thereby improving overall efficiency and productivity (Caldwell, 2009).

Ensuring Security. Information and system security is one of the most critical priorities for modern organizations. In this context, ensuring security is not limited to preventing unauthorized access; it also encompasses maintaining data integrity, implementing security policies and standards, securing system and network infrastructure, regularly evaluating disaster recovery and business continuity plans, and taking proactive measures against cyber threats. An effective security approach ensures the protection of both organizational data and user information, guaranteeing that operational processes continue uninterrupted and securely (Beretas, 2024; Bilgin, 2016).

Figure 1: Ensuring Security

Prevention of Unauthorized Access. Unauthorized access may occur through both internal and external threats. To manage such risks, the implementation of access control mechanisms is essential. Technologies such as encryption, user authentication systems, and multi-factor authentication are used to restrict access to information systems solely to authorized individuals (Bilgin, 2016). In addition, establishing an effective identity management policy within organizations requires the regular review of access rights and the revocation of unnecessary access permissions (Ghadge, 2024). *Protection of Data Integrity*. Data integrity refers to the protection of information against unauthorized modification or deletion. IT auditing applies various tests to identify vulnerabilities that threaten the integrity of systems and databases. For example, file integrity monitoring tools and data validation mechanisms ensure the accuracy of information systems. Such measures support the proper functioning of systems and minimize operational errors (Küçükgergerli & Sarıdoğan, 2022).

Implementation of Security Policies and Standards. IT auditing evaluates the effectiveness of an organization's security policies and standards. A robust information security policy should be developed in accordance with organizational requirements and be clearly understood by all employees. For instance, the ISO/IEC 27001 standard is widely recognized as a global reference for information security management systems and provides guidance for the effective implementation of security controls (Bilgin, 2016).

System and Network Security. Information systems generally involve the integration of multiple networks and systems. Therefore, firewalls, intrusion detection systems, and regular security testing should be employed to ensure network security. In addition, systems must be protected with up-to-date patches, and vulnerabilities in operating systems should be regularly analyzed. IT auditing assists in establishing a defense line against potential threats by evaluating the protection levels of these systems (Küçükgergerli & Sarıdoğan, 2022).

Evaluation of Disaster Recovery and Business Continuity Plans. The effectiveness of disaster recovery and business continuity plans is of critical importance in ensuring the security of information systems. These plans enable organizations to continue their operations without interruption in the event of data loss or system failures. IT auditing evaluates the adequacy of these plans and aims to ensure that they are kept up to date in order to maintain operational capacity (Bilgin, 2016).

Protection Against Cyber Threats. With the advancement of technology, the number and complexity of cyber threats are increasing. IT auditing evaluates an organization's defensive capabilities against cyberattacks and examines whether the necessary measures have been implemented. For example, attack simulations and penetration testing can help identify and mitigate security vulnerabilities (Küçükgergerli & Sarıdoğan, 2022).

Ensuring the security of information systems aims to protect organizations against both internal and external threats and to guarantee the uninterrupted operation of these systems. Preventing unauthorized access, maintaining data integrity, enforcing security policies, and ensuring business continuity in the event of disasters constitute the fundamental pillars of this objective. IT auditing not only identifies deficiencies in these areas but also proposes concrete steps for improvement. In this context, security is regarded not merely as a technical requirement but as a critical component of organizational success.

Conclusion

The relationship between Information Systems and Information Technologies constitutes a fundamental pillar of modern organizational effectiveness. While information systems provide the structural framework for managing data, processes, and human interaction, information technologies supply the technical infrastructure that enables these systems to function efficiently. When aligned strategically, IS and IT not only enhance operational efficiency and decision-making capabilities but also contribute directly to achieving organizational goals.

However, the effectiveness of this relationship is highly dependent on the security of information systems. As organizations increasingly rely on integrated digital infrastructures, they become more vulnerable to internal and external threats. In this context, IT auditing plays a critical role in evaluating

access controls, data integrity, security policies, system and network protections, disaster recovery mechanisms, and cyber defense capabilities. These controls ensure the confidentiality, integrity, and availability of information, which are essential for sustainable operations.

Ultimately, ensuring information system security should not be viewed solely as a technical obligation but as a strategic and organizational necessity. By proactively identifying vulnerabilities and implementing robust security measures, organizations can safeguard their information assets, maintain business continuity, and strengthen their overall resilience in an increasingly complex digital environment.

References

1. Ammanah, C.I. (2024). Development and deployment of a security information management system for enhanced organizational safety and efficiency. *International Journal of Convergent and Informatics Science Research.*
2. Beretas, C. (2024). Information systems security, detection and recovery from cyberattacks. *Universal Library of Engineering Technology, 1*(1).
3. Bilgin, B.Ö. (2016). *Bilgi teknolojileri denetimi ve bir uygulama.*
4. Caldwell, F. (2009, October). Selecting and applying GRC frameworks and standards. In *Gartner Symposium ITExpo*.
5. Crowston, K., Myers, M.D. (2004). Information technology and the transformation of industries: three research perspectives. *The Journal of Strategic Information Systems, 13*(1), 5–28.
6. Dragomir, R.G. (2017). The audit of the quality control system within the information technology field. *Journal of Economic Development, Environment and People, 6*(2), 45–54.
7. Ghadge, N. (2024). Enhancing identity management: Best practices for governance and administration. *Computer Science & Information Technology (CS & IT)*, 219–228.
8. Küçükgergerli, N. & Sarıdoğan, A.A. (2022). The impact of IT application control on the quality of the audit evidence: An application example. *Muhasebe Enstitüsü Dergisi, (66)*, 65–77.
9. Laudon, K.C. & Laudon, J.P. (2020). *Management information systems: Managing the digital firm.* Pearson.
10. Nguyen, A.H., Ha, H.H. & Nguyen, S.L. (2020). Determinants of information technology audit quality: Evidence from Vietnam. *Journal of Asian Finance, Economics and Business, 7*(4), 41–50.
11. Yoon, K., Hoogduin, L. & Zhang, L. (2015). Big data as complementary audit evidence. *Accounting Horizons, 29*(2), 431–438.
12. Zhang, X., Xu, Y.Y. & Ma, L. (2023). Information technology investment and digital transformation: The roles of digital transformation strategy and top management. *Business Process Management Journal, 29*(2), 528–549.

Received: 27.11.2025
Approved: 02.03.2026