Cost Optimization Through Quality Management for a Sustainable IT Company

József Till,[1] Szilvia Erdeiné Késmárki-Gally,[2]
Judit Bernadett Vágány[3]

[1] Hungarian University of Agriculture and Life Sciences, Doctoral School of Economics and Regional Sciences, Gödöllő, Hungary
till.jozsef@phd.uni-mate.hu

[2] Hungarian University of Agriculture and Life Sciences, Institute of Technology, Gödöllő, Hungary
erdeine.kesmarki-gally.szilvia@uni-mate.hu

[3] Budapest University of Economics and Business, Faculty of Commerce, Hospitality and Tourism, Budapest, Hungary
vagany.judit@uni-bge.hu

DOI
https://doi.org/10.18690/um.epf.5.2025.50

ISBN
978-961-286-984-7

Numerous studies support the notion that quality management plays a crucial role in enhancing economic efficiency, particularly through cost reduction and the optimization of operational processes. Companies operating in the IT sector typically focus on compliance with the ISO 27001 and ISO 20000 management systems. Additionally, in recent years, the emergence of frameworks such as NIS 2, DORA, and ESG has introduced new challenges for industry stakeholders. It is also essential to mention ITIL, which serves as the repository of "best practices," as the proper implementation of this system significantly influences the efficiency and quality of IT services. The aim of this publication is to compare and examine the requirements of the standards and frameworks, assessing their impact on cost reduction and efficiency improvement in quality management, as well as their effects on the sustainability of management systems. The risks and opportunities associated with these frameworks are analyzed using secondary research, answering my research questions through the review of relevant academic literature. The expected findings of this research suggest that integrating these new regulations and frameworks into corporate strategy not only facilitates legal compliance but also contributes to cost reduction and process efficiency improvement in the long term.

Keywords:
management system, efficiency, sustainability, legal requirements, cost reduction

JEL:
D24, L15, Q56

University of Maribor Press

1 Introduction

In the modern business world, cybersecurity and the associated improvement of service quality play an increasingly significant role in the operations of IT companies as well. For larger enterprises, the implementation and adherence to standards such as ISO 27001 and ISO 20000 are not uncommon. In 2022, a new edition of the ISO 27001 standard (ISO/IEC 27001:2022, 2022) was released, introducing a completely revised annex and numerous new compliance requirements. Beside that, a growing proportion of IT companies utilize the ITIL (Information Technology Infrastructure Library) framework, which is closely linked to the ISO 20000 standard (ISO/IEC 20000-1:2018, 2018) family (Arraj, 2010). However, the development of cybersecurity and the establishment, support, and enhancement of IT service management alone do not necessarily guarantee the effective operation of quality management. As a result, untapped efficiency reserves may exist within the company's operations.

New European Union regulations have imposed additional obligations on these companies. IT service providers as third party to banking clients affected by the Digital Operational Resilience Act (DORA) (REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, 2022). Over the past decades, the application of information and communication technologies (ICT) has played a pivotal role in financial services, to the extent that it has become indispensable to the daily operations of financial institutions. In parallel, NIS2 regulations have been released by the European Union, which requires strengthening the cybersecurity of the member states (DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, 2022). With that, the government is going to control and monitor such activities, which means high focus at IT companies to fulfill the requirements.

Beyond regulatory requirements, the Environmental, Social, and Governance (ESG) framework has also emerged as a key consideration. The integration of ESG principles into the IT industry is not only important from ethical and legal perspectives but also offers a competitive advantage (Armstrong & McLaren, 2022).

To summarize my key research questions, I am looking for risk and opportunities for the following:

1. How does the integration of ISO 27001 and ISO 20000 enhance IT service quality and cybersecurity resilience?
2. In what ways does compliance with evolving regulations such as DORA and NIS2 increase operational complexity while improving risk management in IT companies?
3. How do organizations that align IT service management with ESG principles gain a competitive advantage and improve stakeholder trust?

2 Theoretical Background

The foundation of every management system comes from the need for quality. Basically, quality management focuses on profit orientation, therefore cost optimization is key for success. The concept of quality costing was first introduced by Juran (1951) in his Quality Control Handbook, where he defined quality costs as "the costs which would disappear if no defects were produced" (Juran, 1951). The challenge lies in determining the optimal quality level that minimizes the total cost of quality (Schiffauerova and Thomson, 2006). Sturm, Kaiser, and Hartmann (2019) explore the long-term relationship between cost of quality and quality performance, emphasizing the importance of sustained investment in quality management to reduce costs over time. Similarly, Fok, Fok, and Hartman (2001) analyzed the role of Total Quality Management (TQM) in information systems development, demonstrating that TQM principles enhance IT efficiency and effectiveness.

In the IT industry, the P-A-F model could be a highly useful tool, comprising the elements of prevention, appraisal, and failure analysis. Vakilifard and Khozein (2012) analyze the four major cost categories in quality management.

These principles led to more complex IT specific requirements; the ISO 27001 standard. While ISO/IEC 27001 and ISO 9001 (ISO 9001:2015, 2015) serve distinct purposes, they can work together to enhance organizational performance. This integration fosters trust, strengthens resilience, and enhances competitive positioning in the market. (Hyseni, 2025)

With the improving cybersecurity and data privacy, new regulations released by the European Union. Firstly the DORA (Digital Operational Resilience Act) came into effect which affects the third party ICT suppliers of the banking sector (2022). This act is determined to have disaster recovery planning and business impact analysis, therefore it is a kind of combined version of ISO 27001 and ISO22301 standards. Beside that, NIS2 (Network and Information System) EU directive was released which requires developing the capability of cybersecurity resilience of each member state. This directive has a similar approach to the quality management system regarding the senior management accountability and the top-down approach. (2022) In addition, it requires the establishment of a Cybersecurity Incident Response Team to manage all the upcoming issues and risks, which eventually increases the overall IT controls.

For further support to improve the service level quality, ITIL (IT Infrastructure Library) and ISO 20000 can provide the proper guidance. ITIL and ISO 20000 are key frameworks in IT service management (ITSM). ITIL standardizes IT service processes, improving efficiency and adaptability across industries (Arraj, 2010; Cervone, 2008). ISO 20000 builds on ITIL principles, offering a structured certification process for compliance and quality assurance. Sahibudin, Sharifi, and Ayat (2008) highlight the integration of ISO 20000 with ITIL, COBIT, and ISO/IEC 27001 for a robust IT governance framework. ITIL's flexibility allows organizations to tailor IT service management strategies, while ISO 20000 ensures accountability and consistency. Popli and Chauhan (2014) emphasize aligning ITSM with agile methodologies to enhance service delivery. Combining both frameworks enhances operational efficiency, regulatory compliance, and service quality.

To achieve the optimized process efficiency and sustainability, IT companies are key players in global net-zero transitions. They are required to have strategies to reduce carbon footprints (Armstrong & McLaren, 2022). Markard and Rosenbloom (2022) outline various phases of the net-zero transition, emphasizing the importance of policy frameworks and technological innovation in achieving sustainability. Furthermore, Environmental, Social, and Governance (ESG) considerations are becoming increasingly significant in the IT sector, influencing corporate sustainability strategies. Organizations are implementing energy-efficient data centers, responsible e-waste management, and ethical AI development to align with ESG principles. ESG in IT is a critical factor in achieving sustainability goals. By

integrating net- zero strategies and responsible IT practices, organizations can enhance environmental responsibility while fostering long-term business resilience.

To encapsulate the core of my research inquiries, this study aims to identify and analyze the associated risks and opportunities pertaining to the following questions:

- How does the integration of ISO 27001 and ISO 20000 enhance IT service quality and cybersecurity resilience?
- In what ways does compliance with evolving regulations such as DORA and NIS2 increase operational complexity while improving risk management in IT companies?
- How do organizations that align IT service management with ESG principles gain a competitive advantage and improve stakeholder trust?

3 Methodology and Results

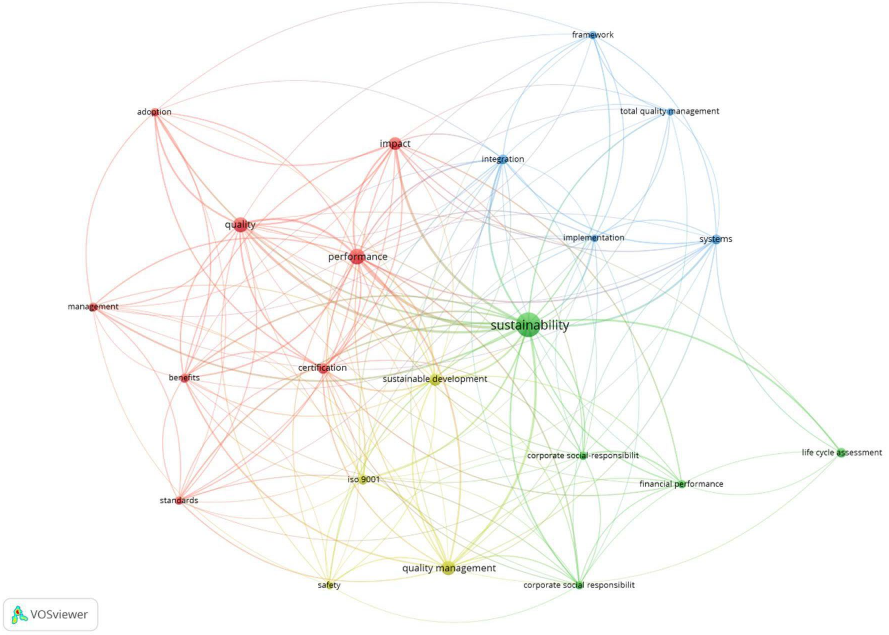

Figure 1: A heatmap - VOSviewer

To prepare the topic of the conference paper by secondary research, I used to collect all the necessary keywords to build a comprehensive search query through the Web of Science. After the search query launched, I collected and stacked the full articles with Notepad++. To filter the relevant topics, I used that stacked file in VOSviewer to create a heatmap with the keywords as showed on figure 1. Eventually, I started to process scientific articles based on my narrowed research area.

To start with, the intersection of quality management, IT service frameworks, cybersecurity regulations, and ESG considerations presents both risks and opportunities which provides answers for the research questions.

As the key risk, optimizing quality while controlling costs is challenging; underinvestment leads to defects, while overinvestment may not be cost-effective (Schiffauerova & Thomson, 2006; Sturm et al., 2019). Poor prevention efforts result in costly internal and external failures (Vakili Fard & Khozein, 2012), increasing cybersecurity threats and reputational damage. Adapting to evolving frameworks like DORA and NIS2 while aligning ISO 9001 and ISO/IEC 27001 poses operational challenges (Hyseni, 2025). Integrating ITIL and ISO 20000 requires balancing flexibility with compliance (Sahibuddin et al., 2008; Popli & Chauhan, 2014).

On the opportunities side, TQM and structured ITSM lower long-term costs and enhance efficiency (Fok et al., 2001; Sturm et al., 2019). Combining ISO 20000, ITIL, and cybersecurity frameworks improves compliance and risk management (Sahibuddin et al., 2008). Net-zero initiatives and responsible IT practices boost corporate reputation and resilience (Armstrong & McLaren, 2022; Markard & Rosenbloom, 2022). Standardized ITSM enhances reliability and customer trust, while agile integration increases adaptability (Arraj, 2010; Cervone, 2008; Popli & Chauhan, 2014).

4 Discussion

The findings suggest that IT organizations must adopt a proactive approach to quality management by integrating ITSM frameworks, cybersecurity standards, and regulatory compliance. The interplay between ITIL, ISO 20000, and ISO 27001 presents a unique opportunity for companies to establish a comprehensive quality management system at a sustainable IT company. However, the challenge lies in

balancing flexibility with compliance, especially in rapidly evolving regulatory landscapes such as DORA and NIS2. ESG considerations further complicate IT quality management, requiring organizations to align sustainability goals with operational efficiency.

Moreover, organizations must recognize the significance of a risk-based approach when implementing and maintaining a quality management framework in parallel with other IT specific systems. Therefore, companies must develop adaptive compliance strategies that address emerging threats while maintaining operational resilience. Additionally, the alignment of ITSM with ESG policies requires organizations to incorporate sustainability metrics into their performance assessments, ensuring that environmental and social responsibilities are integrated into IT operations.

Ultimately, secondary research highlights the necessity of a holistic approach to IT quality management, where regulatory compliance, cybersecurity, and sustainability are interwoven into a single strategic vision. Organizations that successfully navigate this complex landscape will be better positioned to foster innovation, enhance customer trust, and sustain long-term growth.

5 Conclusions

The research conducted provides valuable insights into the integration of ISO 27001 and ISO 20000, compliance with evolving regulations such as DORA and NIS2, and the alignment of IT service management with ESG principles.

Firstly, the integration of ISO 27001 and ISO 20000 significantly enhances IT service quality and cybersecurity resilience. By combining these standards, organizations can establish a robust framework that ensures the protection of information assets while maintaining high service quality. This integration promotes trust, strengthens resilience, and enhances competitive positioning in the market.

Secondly, compliance with evolving regulations such as DORA and NIS2 increases operational complexity but also improves risk management in IT companies. The Digital Operational Resilience Act (DORA) and the Network and Information System (NIS2) directive require organizations to develop comprehensive disaster

recovery plans, business impact analysis, and cybersecurity resilience capabilities. These regulations necessitate a top-down approach to quality management, ensuring senior management accountability and the establishment of a Cybersecurity Incident Response Team to manage risks effectively.

Lastly, organizations that align IT service management with ESG principles gain a competitive advantage and improve stakeholder trust. The integration of Environmental, Social, and Governance (ESG) considerations into IT operations is crucial for achieving sustainability goals. By implementing energy-efficient data centers, responsible e-waste management, and ethical AI development, organizations can enhance their environmental responsibility while fostering long-term business resilience.

Despite the valuable insights provided, this research has several limitations. Firstly, the study relies heavily on secondary data, which may not capture the most recent developments in the field. Additionally, the research focuses primarily on large enterprises, potentially overlooking the unique challenges faced by smaller IT companies. The study also assumes a uniform environmental impact. Moreover, IT firms must integrate ESG considerations into their supply chains, ensuring ethical sourcing of materials, reducing emissions from cloud and data center operations, and enhancing circular economy principles. The adoption of renewable energy in IT infrastructure, alongside energy-efficient data centers, plays a crucial role in achieving Net Zero ambitions while maintaining cost-effective IT services.

References

Armstrong, C., & McLaren, D. (2022). Which Net Zero? Climate Justice and Net Zero Emissions. *Ethics & International Affairs,* 36(4), 505–526. https://doi.org/10.1017/S0892679422000521

Arraj, V. (2010). *ITIL®: the basics.* Buckinghampshire, UK.

Cervone, F. (2008). ITIL: a framework for managing digital library services. *OCLC Systems & Services: International digital library perspectives*, 24(2), 87-90. https://doi.org/10.1108/10650750810875430

COUNCIL (2022), https://eur-lex.europa.eu/legal- content/HU/TXT/?uri=CELEX:32022R2554

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (2022),

Fok, L. Y., Fok, W. M., & Hartman, S. J. (2001). Exploring the relationship between total quality management and information systems development. *Information & Management,* 38(6), 355-371. https://doi.org/10.1016/S0378-7206(00)00075-6

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

https://pecb.com/article/isoiec-27001-vs-iso-9001-key-differences-and-similarities

Hyseni, V. (2025, March 3) *ISO/IEC 27001 vs ISO 9001: Key Differences and Similarities*

ISO 9001:2015, *Quality management systems — Requirements* (2015), https://www.iso.org/standard/62085.html

ISO/IEC 20000-1:2018, *Information technology — Service management* (2018), https://www.iso.org/standard/70636.html

ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (2022), https://www.iso.org/standard/27001

Juran, J.M. (1951). *Quality Control Handbook, 1st ed.*, McGraw-Hill.

Markard, J., & Rosenbloom, D. (2022). Phases of the net-zero energy transition and strategies to achieve it. *In Routledge handbook of energy transitions*, 102-123. Routledge.

Popli, R., & Chauhan, N. (2014, February). Cost and effort estimation in agile software development. *In 2014 international conference on reliability optimization and information technology (ICROIT)*, 57-61. IEEE. https://doi.org/10.1109/ICROIT.2014.6798284

REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE

Sahibuddin, S., Sharifi, M., & Ayat, M. (2008, May). Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations. *In 2008 Second Asia International Conference on Modelling & Simulation (AMS),* 749-753. IEEE.

Schiffauerova, A. and Thomson, V. (2006), "A review of research on cost of quality models and best practices", *International Journal of Quality & Reliability Management,* Vol. 23 (No. 6), 647-669. https://doi.org/10.1108/02656710610672470

Sturm, S., Kaiser, G., & Hartmann, E. (2019). Long-run dynamics between cost of quality and quality performance. *International Journal of Quality & Reliability Management,* 36(8), 1438- 1453. https://doi.org/10.1108/IJQRM-05-2018-0118

Vakilifard, H., & Khozein, A. (2012). Prevention, Appraisal, Internal failure, external failure cost and Quality Optimization. *Journal of Mathematics and Computer Sciences*, 10, 539-551.